Cambium Point-to-Multipoint (PMP) Solutions User Guide

System Release 11.2

Cambium Networks

Cambium module essential information

Default IP Address for Management GUI Access	169.254.1.1
Default Administrator Username	admin
Default Administrator Password	(no password)
Software Upgrade Procedure	See Using the Canopy Network Updater Tool (CNUT) on page 499
Resetting to Factory Defaults (2 options)	1. On the radio GUI, navigate to **Configuration**, **Unit Settings** and select **Set to Factory Defaults** ***OR*** 2. On the radio GUI, navigate to **Configuration**, **Unit Settings** and enable and save option **Set to Factory Defaults Upon Default Plug Detection**. When the unit is powered on with a default/override plug the radio will be returned to its factory default settings.

Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Cambium Networks assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party Software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Components, units, or 3rd Party products used in the product described herein are NOT fault-tolerant and are NOT designed, manufactured, or intended for use as on-line control equipment in the following hazardous environments requiring fail-safe controls: the operation of Nuclear Facilities, Aircraft Navigation or Aircraft Communication Systems, Air Traffic Control, Life Support, or Weapons Systems (High Risk Activities). Cambium and its supplier(s) specifically disclaim any expressed or implied warranty of fitness for such High Risk Activities.

© 2013 Cambium Networks, Inc. All Rights Reserved.

Contents

Cambium module essential information 2

Chapter 1: About this User Guide 20

Portfolio of Wireless Broadband Solutions 23

Products Covered by This User Guide 23

Products Not Covered by This User Guide 24

Software Compatibility Described in This User Guide 24

Chapter 2: Using This User Guide 25

Finding the Information You Need 25

Becoming Familiar with This User Guide 25

Searching This User Guide 28

Interpreting Typeface and Other Conventions 28

Sending Feedback 30

Chapter 3: Advancing from Research to Implementation 32

Chapter 4: Realizing a Wireless Ethernet Bridge Network 33

Chapter 5: Exploring the Scope of Solutions 35

Product Names 35

Network Components 36

Access Point Module Other Than 900-Mhz 36

Access Point Cluster 37

Subscriber Module Other Than 900-MHz 37

900-MHz AP and SM 38

PTP Series 100 Bridges 40

PTP 200 Series Bridges 41

PTP 300 Series Bridges 41

PTP 400 Series Bridges 41

PTP 500 Series Bridges 42

PTP 600 Series Bridges 42

PTP 800 Series Bridges 44

PTP 810/810i Series Bridges 45

Radio Adjustable Power Capabilities 46

Cluster Management Module-2 (Part 1008CK-2) 47

Cluster Management Module micro (Part 1070CK) 47

CMM4 (Part 1090CK, 1091AA) 49

Optional Ethernet Switch in CMM4 - (Part 1090CK, 1091AA) 50

Rackmount CMM4 (1092AA) 51

GPS Antenna (Part GPSANTPNM03D) 52

UNIVERSAL GPS (UGPS) 53

Surge Suppressor (Part 600SS) 53

Accessory Components 54
Frequency Band Ranges 60
Product Comparisons 61
Product Applications 61
Link Performance and Encryption Comparisons 62
Cluster Management Product Comparison 66
Antennas for 900-MHz Connectorized Modules 67
Adjunctive Software Products 69
Wireless Manager (WM) 70
Prizm 71
Network Definition and Element Discovery 71
Monitoring and Fault Management 72
Element Management 72
Northbound Interface 73
License Management 73
Specifications and Limitations 75
Radios 75
Cluster Management Products 75
600SS Surge Suppressor 75
Chapter 6: Differentiating Among Components 76
Interpreting Model Number 76
Sorted Model Numbers 78
Interpreting Electronic Serial Number (ESN) 80
Finding the Model (Part) Number and ESN 80
Chapter 7: Link Characteristics 81
Understanding Bandwidth Management 81
Downlink Frame 81
Uplink Frame 81
Slot Calculation 82
Startup Sequence 82
Data Transfer Capacity 83
Maximum Information Rate (MIR) Parameters 83
Token Bucket Algorithm 83
MIR Data Entry Checking 84
Committed Information Rate 85
Bandwidth from the SM Perspective 85
Interaction of Burst Allocation and Sustained Data Rate Settings 86
High-priority Bandwidth 86
Traffic Scheduling 88
2X Operation 89
3X Operation 92
Engineering for 2X and 3X Operation 93
Understanding Synchronization 94
GPS Synchronization 94

Passing Sync in a Single Hop 96
Passing Sync in an Additional Hop 96
Chapter 8: Meeting Link Requirements 99
AP-SM Links 99
BH-BH Links 101
Chapter 9: Previewing Network Configurations 102
Viewing Typical Layouts 102
Chapter 10: Accessing Features 104
Activating Features 114
Fixed License Keys 114
Enabling Features 114
Chapter 11: Acquiring Proficiencies 115
Understanding RF Fundamentals 115
Understanding IP Fundamentals 115
Acquiring a Demonstration Kit 115
900-MHz with Integrated Antenna and Band-pass Filter Demonstration Kit 115
900-MHz with Connectorized Antenna Demonstration Kit 116
2.4-GHz with Adjustable Power Set to High Demonstration Kit 116
5.2-GHz Demonstration Kit 117
5.4-GHz Demonstration Kit 118
5.7-GHz with Connectorized Antenna and Adjustable Power Set to Low Demonstration Kit 118
Demonstration Kit Part Numbers 119
Acquiring a Starter Kit 119
900-MHz with Integrated Antenna and Band-pass Filter Starter Kit 119
900-MHz with Connectorized Antenna Starter Kit 120
2.4-GHz with Adjustable Power Set to High Starter Kit 120
5.2-GHz Starter Kit 120
5.4-GHz FSK Starter Kit 121
5.4-GHz OFDM Starter Kits 121
5.7-GHz with Integrated Antenna Starter Kit 122
Starter Kit Part Numbers 122
Chapter 12: Engineering Your RF Communications 123
Anticipating RF Signal Loss 123
Understanding Attenuation 123
Calculating Rx Signal Level 124
Calculating Fade Margin 124
Analyzing the RF Environment 125
Mapping RF Neighbor Frequencies 125
Anticipating Reflection of Radio Waves 126
Noting Possible Obstructions in the Fresnel Zone 127
Radar Signature Detection and Shutdown 127
Using Jitter to Check Received Signal Quality (FSK Only) 131
Using Link Efficiency to Check FSK Received Signal Quality 132
Comparing Efficiency in 1X Operation to Efficiency in 2X Operation 133

When to Switch from 2X to 1X Operation Based on 60% Link Efficiency 133
Considering Frequency Band Alternatives 134
900-MHz Channels 135
2.4-GHz Channels 135
4.9-GHz OFDM Channels 136
5.2-GHz Channels 136
5.4-GHz FSK Channels 137
5.4-GHz OFDM Channels 138
5.7-GHz Channels 139
Channels Available for PTP 400 and PTP 600 Radios 140
Example Channel Plans for FSK AP Clusters 140
Multiple FSK Access Point Clusters 142
Multiple OFDM Access Point Clusters 143
Selecting Sites for Network Elements 144
Surveying Sites 145
Assuring the Essentials 145
Clearing the Radio Horizon 147
Calculating the Aim Angles 148
Co-locating Modules 149
Deploying a Remote AP 150
Remote AP Performance 151
Example Use Case for RF Obstructions 152
Example Use Case for Passing Sync 153
Physical Connections Involving the Remote AP 153
Diagramming Network Layouts 154
Accounting for Link Ranges and Data Handling Requirements 154
Avoiding Self Interference 154
Avoiding Other Interference 156
Chapter 13: Engineering Your IP Communications 157
Understanding Addresses 157
IP Address 157
Dynamic or Static Addressing 157
When a DHCP Server is Not Found 158
Network Address Translation (NAT) 158
NAT, DHCP Server, DHCP Client, and DMZ in SM 158
NAT and VPNs 163
Developing an IP Addressing Scheme 164
Address Resolution Protocol 164
Allocating Subnets 164
Selecting Non-routable IP Addresses 165
Translation Bridging 165
Chapter 14: Engineering VLANs 167
Special Case VLAN Numbers 167
SM Membership in VLANs 168

Priority on VLANs (802.1p) 169
Q-in-Q DVLAN (Double-VLAN) Tagging (802.1AD) 169
Chapter 15: Avoiding Hazards 174
Exposure Separation Distances 174
Details of Exposure Separation Distances Calculations and Power Compliance Margins 175
Grounding the Equipment 177
Grounding Infrastructure Equipment 177
Grounding SMs 178
Conforming to Regulations 181
Protecting Cables and Connections 181
Chapter 16: Testing the Components 183
Unpacking Components 183
Configuring for Test 183
Configuring the Computing Device for Test 183
Default Module Configuration 184
Component Layout 184
Diagnostic LEDs 185
Standards for Wiring 187
Best Practices for Cabling 187
Recommended Tools for Wiring Connectors 187
Wiring Connectors 188
Alignment Tone—Technical Details 189
Configuring a Point-to-Multipoint Link for Test 190
Quick Start Page of the AP 191
Time Tab of the AP 198
Session Status Tab of the AP 200
Beginning the Test of Point-to-Multipoint Links 206
Remote Subscribers Tab of the AP 206
General Status Tab of the SM 207
Continuing the Test of Point-to-Multipoint Links 212
General Status Tab of the AP 212
Concluding the Test of Point-to-Multipoint Links 218
Configuring a Point-to-Point Link for Test 218
Quick Start Page of the BHM 219
Time Tab of the BHM 221
Beginning the Test of Point-to-Point Links 223
Continuing the Test of Point-to-Point Links 228
General Status Tab of the BHM 229
Concluding the Test of Point-to-Point Links 233
Chapter 17: Preparing Components for Deployment 234
Correlating Component-specific Information 234
Ensuring Continuing Access to the Modules 234
Chapter 18: Configuring for the Destination 236
Configuring an AP for the Destination 236

General Tab of the AP 236
IP Tab of the AP 242
Radio Tab of the AP 245
SNMP Tab of the AP 255
Quality of Service (QoS) Tab of the AP 258
Security Tab of the AP 261
VLAN Tab of the AP 265
VLAN Membership Tab of the AP 269
Diffserv Tab of the AP 270
Protocol Filtering Tab of the AP 272
Unit Settings Tab of the AP 274
Configuring an SM for the Destination 277
General Tab of the SM 277
NAT and IP Tabs of the SM with NAT Disabled 280
NAT and IP Tabs of the SM with NAT Enabled 287
Radio Tab of the SM 294
SNMP Tab of the SM 298
Quality of Service (QoS) Tab of the SM 302
Security Tab of the SM 305
VLAN Tab of the SM 308
VLAN Membership Tab of the SM 314
Diffserv Tab of the SM 314
Protocol Filtering Tab of the SM 317
PPPoE Tab of the SM 318
NAT Port Mapping Tab of the SM 322
Unit Settings Tab of the SM 322
Setting the Configuration Source 324
Configuring a BH Timing Master for the Destination 327
General Tab of the BHM 327
IP Tab of the BHM 331
Radio Tab of the BHM 334
SNMP Tab of the BHM 339
Security Tab of the BHM 343
VLAN tab of the BHM 346
DiffServ Tab of the BHM 349
Protocol Filtering Tab of the BHM 352
Unit Settings Tab of the BHM 354
Configuring a BH Timing Slave for the Destination 355
General Tab of the BHS 356
IP Tab of the BHS 360
Radio Tab of the BHS 363
SNMP Tab of the BHS 366
Quality of Service (QoS) Tab of the BHS 370
Security Tab of the BHS 370

VLAN Tab of the BHS 372
Diffserv Tab of the BHS 375
Protocol Filtering Tab of the BHS 378
Unit Settings Tab of the BHS 380
Adjusting Transmitter Output Power 382
Chapter 19: Installing Components 385
PDA Access to Modules 385
Installing an AP 386
Installing a PMP 100 Series AP 386
Installing a PMP 400 Series AP 386
Installing a Connectorized Flat Panel Antenna 392
Weatherproofing a 900 MHz Connectorized Antenna 394
Installing a GPS Antenna 395
Installing a Cluster Management Module 395
Installing an SM 395
Configuring the Laptop for Connection to SMs 395
Installing a PMP 100 Series SM 397
Installing a PMP 400 Series SM 402
Configuring an AP-SM Link 404
Monitoring an AP-SM Link 406
Installing a Reflector Dish 408
Both Modules Mounted at Same Elevation 408
Modules Mounted at Different Elevations 409
Mounting Assembly 409
Installing a BH Timing Master 410
Installing a PTP 100 Series BHM 410
Installing a PTP 200 Series BHM 412
Installing a BH Timing Slave 412
Installing a PTP 100 Series BHS 412
Installing a PTP 200 Series BHS 414
Upgrading a BH Link to BH20 414
Verifying a BH Link 415
Chapter 20: Verifying System Functionality 417
Chapter 21: Growing Your Network 420
Monitoring the RF Environment 420
Spectrum Analyzer 420
Graphical Spectrum Analyzer Display 421
Using the AP as a Spectrum Analyzer 422
Considering Software Release Compatibility 425
Designations for Hardware in Radios 425
MIB File Set Compatibility 426
Redeploying Modules 426
Wiring to Extend Network Sync 426
Chapter 22: Securing Your Network 428

Isolating APs from the Internet 428
Encrypting Radio Transmissions 428
DES Encryption 428
AES Encryption 429
AES-DES Operability Comparisons 429
Managing Module Access by Passwords 430
Adding a User for Access to a Module 430
Deleting a User from Access to a Module 432
Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH 433
Requiring SM Authentication 435
Filtering Protocols and Ports 435
Port Filtering with NAT Enabled 436
Protocol and Port Filtering with NAT Disabled 436
Encrypting Downlink Broadcasts 438
Isolating SMs 438
Filtering Management through Ethernet 438
Allowing Management from Only Specified IP Addresses 439
Configuring Management IP by DHCP 439
Chapter 23: Managing Bandwidth and Authentication 440
Managing Bandwidth without RADIUS, Prizm, or BAM 440
Bandwidth and Authentication Manager (BAM) Services and Features 440
Bandwidth Manager Capability 441
Authentication Manager Capability 442
Chapter 24: Configuring a RADIUS server 444
Understanding RADIUS 444
RADIUS Functions 444
Tested RADIUS Servers 444
Choosing Authentication Mode and Configuring for Authentication Servers - AP 445
SM Authentication Mode – Require RADIUS or Follow AP 447
Handling Certificates 449
Configuring your RADIUS servers for SM authentication 451
Configuring your RADIUS server for SM configuration 451
Assigning SM management IP addressing via RADIUS 452
Using RADIUS for centralized AP and SM user name and password management 454
RADIUS Attribute Framed-IP-Address 458
Chapter 25: Managing the Network From a Management Station (NMS) 459
Roles of Hardware and Software Elements 459
Role of the Agent 459
Role of the Managed Device 459
Role of the NMS 459
Dual Roles for the NMS 460
Simple Network Management Protocol (SNMP) Commands 460
Traps from the Agent 460
AP SNMP Proxy to SMs 460

Management Information Base (MIB) 463
Cascading Path to the MIB 463
Object Instances 464
Management Information Base Systems and Interface (MIB-II) 464
Canopy Enterprise MIB 465
Configuring Modules for SNMP Access 466
Objects Defined in the Canopy Enterprise MIB 467
AP, SM, and BH Objects 467
AP and BH Timing Master Objects 481
SM and BH Timing Slave Objects 488
Interface Designations in SNMP 496
Traps Provided in the Canopy Enterprise MIB 497
MIB Viewers 497
Chapter 26: Using the Canopy Network Updater Tool (CNUT) 499
CNUT Functions 499
Network Element Groups 499
Network Layers 500
Script Engine 500
Software Dependencies for CNUT 501
CNUT Download 501
Chapter 27: Using Informational Tabs in the GUI 502
Viewing General Status (All) 502
Viewing Session Status (AP, BHM) 502
Viewing Remote Subscribers (AP, BHM) 503
Interpreting Messages in the Event Log (All) 504
Time and Date Stamp 504
Event Log Data Collection 504
Messages that Flag Abnormal Events 505
Messages that Flag Normal Events 506
Viewing the Network Interface Tab (All) 506
Viewing the Layer 2 Neighbors Tab (All) 507
Viewing the Scheduler Tab (All) 507
List of Registration Failures (AP, BHM) 509
Interpreting Data in the Bridging Table (All) 509
Translation Table (SM) 510
Interpreting Data in the Ethernet Tab (All) 511
Interpreting RF Control Block Statistics in the Radio Tab (All) 514
Interpreting Data in the VLAN Tab (All) 515
Viewing Data VC Statistics (All) 516
Viewing Summary Information in the Overload Tab (All) 519
Viewing the DHCP Relay Tab (AP) 520
Viewing Filter Statistics (SM, BHS) 522
Viewing ARP Statistics (SM, BHS) 523
Viewing NAT Statistics (SM) 523

Viewing NAT DHCP Statistics (SM) 525
Interpreting Data in the GPS Status Page (AP, BHM) 526
Accessing PPPoE Statistics About Customer Activities (SM) 527
Viewing Bridge Control Block Statistics (All) 529
Chapter 28: Using Tools in the GUI 532
Using the Spectrum Analyzer Tool (SM, BHS) 532
Using the Alignment Tool (SM, BHS) 532
Using the Link Capacity Test Tool (All) 533
Using the AP Evaluation or BHM Evaluation Tool (SM, BHS) 536
Using the Frame Calculator Tool (All) for Co-location 542
Viewing the DFS Status Tab (All) 547
Using the SM Configuration Tool (AP, BHM) 548
Reviewing the Link Status Tool Results (AP) 549
Using the Remote Spectrum Analyzer Tool (AP) 551
Using the BER Results Tool (SM, BHS) 553
Chapter 29: Maintaining Your Software 555
Typical Contents of Release Notes 555
Typical Upgrade Process 555
Downloading Software and Release Notes 556
Rebranding Module Interface Screens 557
Setting Up a Protocol Analyzer on Your Network 560
Analyzing Traffic at an SM 561
Analyzing traffic at an AP or BH with no CMM 562
Analyzing Traffic at an AP or BH with a CMM 562
Example of a Protocol Analyzer Setup for an SM 563
Chapter 30: Troubleshooting 570
General Planning for Troubleshooting 570
General Fault Isolation Process 570
Questions to Help Isolate the Problem 571
Secondary Steps 571
Procedures for Troubleshooting 572
Module Has Lost or Does Not Establish Connectivity 572
NAT/DHCP-configured SM Has Lost or Does Not Establish Connectivity 573
SM Does Not Register to an AP 574
BHS Does Not Register to the BHM 575
Module Has Lost or Does Not Gain Sync 576
Module Does Not Establish Ethernet Connectivity 576
Module Does Not Power Up 577
Power Supply Does Not Produce Power 578
CMM Does Not Pass Proper GPS Sync to Connected Modules 578
Module Software Cannot be Upgraded 579
Module Functions Properly, Except Web Interface Became Inaccessible 579
Chapter 31: Administering Modules through Telnet Interface 581
Chapter 32: Regulatory and Legal Notices 583

Important Note on Modifications 583
National and Regional Regulatory Notices 583
U.S. Federal Communication Commission (FCC) Notification 583
Industry Canada (IC) Notification 586
Regulatory Requirements for CEPT Member States (www.cept.org) 587
European Union Notification for 5.7 GHz Product 588
Equipment Disposal 589
EU Declaration of Conformity for RoHS Compliance 589
UK Notification 589
Belgium Notification 589
Luxembourg Notification 590
Czech Republic Notification 590
Norway Notification 590
Italy Notification 590
Greece Notification 591
Brazil Notification 591
Australia Notification 591
Labeling and Disclosure Table for China 592
RF Exposure 593
Legal Notices 593
Software License Terms and Conditions 593
Hardware Warranty in U.S. 596
Limit of Liability 596
Chapter 33: Additional Resources 597

List of Figures

Figure 1: Pole-mounted AP cluster 37
Figure 2: OFDM AP - Antenna and Radio 37
Figure 3: Structure-mounted SM 37
Figure 4: OFDM SM, front and side views 38
Figure 5: Examples of antennas for 900-MHz modules 39
Figure 6: Dish-mounted 7.5- or 14-Mbps bridge 40
Figure 7: 21-Mbps bridge 41
Figure 8: PTP 300/400/500/600 Series Bridge common form 41
Figure 9: CMM2 enclosure 47
Figure 10: CMM2 pole-mounted 47
Figure 11: CMMmicro 48
Figure 12: Pole-mounted CMMmicro 48
Figure 13: CMM4 enclosure 50
Figure 14: CMM4 50
Figure 15: Rackmount CMM4 52
Figure 16: Cambium GPS antenna 52
Figure 17: Cambium UGPS antenna 53
Figure 18: 600SS surge suppressor 53
Figure 19: 27RD with mounted module 56
Figure 20: LENS mounted on a radio 56
Figure 21: SMMB1 SM support bracket 57
Figure 22: ACATHS-01 alignment headset 59
Figure 23: HSG-01 Housing 60
Figure 24: TDD dividing frames 83
Figure 25: Uplink and downlink rate caps adjusted to apply aggregate cap 84
Figure 26: Uplink and downlink rate cap adjustment example 85
Figure 27: One unsynchronized AP in cluster 95
Figure 28: GPS timing throughout the network (FSK shown) 96
Figure 29: Additional link to extend network sync, Design 3 97
Figure 30: Additional link to extend network sync, Design 4 97
Figure 31: Additional link to extend network sync, Design 5 98
Figure 32: Typical network layout with no BH 102
Figure 33: Typical network layout with BH 103
Figure 34: Typical multiple-BH network layout 103
Figure 35: Determinants in Rx signal level 124
Figure 36: Example layout of 7 FSK Access Point clusters 142
Figure 37: Example layout of 16 Access Point sectors (ABCD), 90 degree sectors 143
Figure 38: Example layout of 16 Access Point sectors (ABC), 60 degree sectors 144
Figure 39: Fresnel zone in line of sight link 146

Figure 40: Fresnel zone in near line of sight link 146
Figure 41: Fresnel zone in non-line of sight link 147
Figure 42: Variables for calculating angle of elevation (and depression) 148
Figure 43: Double-hop backhaul links 150
Figure 44: Remote AP deployment 151
Figure 45: Example 900-MHz remote AP behind 2.4-GHz SM 152
Figure 46: Remote AP wired to SM that also serves a customer 153
Figure 47: Remote AP wired to SM that serves as a relay 154
Figure 48: NAT Disabled implementation 159
Figure 49: NAT with DHCP Client and DHCP Server implementation 160
Figure 50: NAT with DHCP Client implementation 161
Figure 51: NAT with DHCP Server implementation 162
Figure 52: NAT without DHCP implementation 163
Figure 53: Example of IP address in Class B subnet 165
Figure 54 Q-in-Q network diagram 170
Figure 55: Base cover, detached and attached, FSK module 184
Figure 56: Base cover, detached and attached, OFDM module 185
Figure 57: RJ-45 pinout for straight-through Ethernet cable 188
Figure 58: RJ-45 pinout for crossover Ethernet cable 189
Figure 59: RJ-11 pinout for straight-through sync cable 189
Figure 60: Quick Start tab of AP, example 191
Figure 61: Region Settings tab of AP, example 192
Figure 62: Radio Carrier Frequency tab of AP, example 193
Figure 63: Synchronization tab of AP, example 194
Figure 64: LAN IP Address tab of AP, example 195
Figure 65: Review and Save Configuration tab of AP, example 197
Figure 66: Time tab of AP, example 198
Figure 67: Session Status tab data from AP, example 201
Figure 68: Remote Subscribers tab of AP, example 206
Figure 69: General Status tab of SM, example 207
Figure 70: General Status tab of AP, example 213
Figure 71: Quick Start tab of BHM, example 219
Figure 72: Time tab of BHM, example 221
Figure 73: General Status tab of BHS, example 224
Figure 74: General Status tab of BHM, example 229
Figure 75: General tab of AP, example 237
Figure 76: IP tab of AP, example 242
Figure 77: Radio tab of AP, example 246
Figure 78: SNMP tab of AP, example 255
Figure 79: Quality of Service (QoS) tab of AP, example 258
Figure 80: Security tab of AP, example 261
Figure 81: VLAN tab of AP, example 265
Figure 82: VLAN Membership tab of AP, example 269
Figure 83: Diffserv tab of AP, example 270

Figure 84: Protocol Filtering tab of AP, example 273
Figure 85: Unit Settings tab of AP, example 275
Figure 86: General tab of SM, example 277
Figure 87: NAT tab of SM with NAT disabled, example 281
Figure 88: IP tab of SM with NAT disabled, example 285
Figure 89: NAT tab of SM with NAT enabled, example 288
Figure 90: IP tab of SM with NAT enabled, example 294
Figure 91: Radio tab of SM, example 295
Figure 92: SNMP tab of SM, example 299
Figure 93: Quality of Service (QoS) tab of SM, example 302
Figure 94: Security tab of SM, example 305
Figure 95: VLAN tab of SM, example 309
Figure 96: VLAN Membership tab of SM, example 314
Figure 97: Diffserv tab of SM, example 315
Figure 98: Protocol Filtering tab of SM, example 317
Figure 99: PPPoE tab of SM, example 319
Figure 100: NAT Port Mapping tab of SM, example 322
Figure 101: Unit Settings tab of SM, example 323
Figure 102: General tab of BHM, example 328
Figure 103: IP tab of BHM, example 332
Figure 104: Radio tab of BHM, example 334
Figure 105: SNMP tab of BHM, example 340
Figure 106: Security tab of BHM, example 344
Figure 107: VLAN tab of BHM, example 347
Figure 108: Diffserv tab of BHM, example 350
Figure 109: Protocol Filtering tab of SM, example 353
Figure 110: Unit Settings tab of BHM, example 354
Figure 111: General tab of BHS, example 357
Figure 112: IP tab of BHS, example 361
Figure 113: Radio tab of BHS, example 363
Figure 114: SNMP tab of BHS, example 367
Figure 115: Quality of Service (QoS) tab of BHS, example 370
Figure 116: Security tab of BHS, example 371
Figure 117: VLAN tab of BHS, example 373
Figure 118: Diffserv tab of BHS, example 376
Figure 119: Protocol Filtering tab of SM, example 379
Figure 120: Unit Settings tab of BHS, example 381
Figure 121: Parts inventory for OFDM AP installation 387
Figure 122: Assembled upper bracket for OFDM AP 387
Figure 123: OFDM AP connected to its antenna 388
Figure 124: OFDM AP mounted to its antenna 388
Figure 125: OFDM AP ready for tower mount 389
Figure 126: Hanging OFDM AP assembly onto upper bracket of pole mount 389
Figure 127: OFDM AP attached to pole or tower 390

Figure 128: OFDM antenna lower bracket with quick-connect 390
Figure 129: Ground lug and coaxial cable of OFDM AP 391
Figure 130: Down tilt adjustment bracket of OFDM AP 392
Figure 131: Sealing 900MHz antenna standoffs 394
Figure 132 Sealing between the 900MHz radio and antenna 394
Figure 133: Example Local Area Connection Properties window 396
Figure 134: Example Internet Protocol (TCP/IP) Properties window 396
Figure 135: SM attachment to reflector arm 398
Figure 136: SM grounding per NEC specifications 399
Figure 137: Internal view of Canopy 600SS Surge Suppressor 400
Figure 138: Override plug 401
Figure 139: Audible Alignment Tone kit, including headset and connecting cable 402
Figure 140: Example data from AP Evaluation tab 405
Figure 141: AP/SM link status indications in the AP Session Status tab 407
Figure 142: Correct mount with reflector dish 408
Figure 143: Incorrect mount with reflector dish 409
Figure 144: Mounting assembly, exploded view 410
Figure 145: BH attachment to reflector arm 411
Figure 146: Spectrum Analyzer tab of SM, example 422
Figure 147: General Status tab view for GUEST-level account 431
Figure 148: Add User tab of SM, example 432
Figure 149: Delete User tab of SM, example 432
Figure 150: RJ-11 pinout for the override plug 434
Figure 151: Categorical protocol filtering 437
Figure 152: Security tab of the AP 446
Figure 153: Security tab of the SM 448
Figure 154: SM Certificate Management 450
Figure 155 User Authentication tab of the AP 455
Figure 156 User Authentication tab of the AP 456
Figure 157 User Authentication tab of the SM 457
Figure 158: Session Status tab data, example 503
Figure 159: Event Log tab data, example 505
Figure 160: Network Interface tab of AP, example 506
Figure 161: Layer 2 Neighbors log, example 507
Figure 162: Scheduler tab of the AP 507
Figure 163: SM Registration Failures tab of the AP 509
Figure 164: Bridging Table tab of the AP 509
Figure 165: Translation Table tab of the SM 510
Figure 166: Ethernet tab of AP 511
Figure 167: Radio tab of the Statistics page, SM 514
Figure 168: VLAN tab of the AP 516
Figure 169: Data VC tab of the AP 517
Figure 170: Overload tab of the AP 519
Figure 170: DHCP Relay tab of the AP 521

Figure 171: Filter tab of the SM 522
Figure 172: ARP tab of the SM 523
Figure 173: NAT Stats tab of the SM 523
Figure 174: NAT DHCP Statistics of the SM 525
Figure 175: PPPoE tab of the SM 527
Figure 176: Bridge Control Block statistics 529
Figure 177: Alignment Tool tab of SM, example for a good link 532
Figure 178: Alignment Tool tab of SM, example for an acceptable link 532
Figure 179: Alignment Tool tab of SM, example for an unacceptable link 533
Figure 180: Link Capacity Test tab of AP, example 534
Figure 181: Link Capacity Test tab with 64-byte packet length, example 535
Figure 182: AP Evaluation tab of SM, example 537
Figure 183: Frame Calculator tab, example 544
Figure 184: Calculated Frame Results section of Frame Calculator tab, example 546
Figure 185: DFS Status tab of AP, example 547
Figure 186: SM Configuration tab of AP, example 549
Figure 187: Link Status tab of AP, example 550
Figure 188: Remote Spectrum Analyzer tab of AP, example 552
Figure 189: BER Results tab of FSK SM, example 553
Figure 190: Example ftp session to transfer custom logo file 558
Figure 191: Example telnet session to activate custom logo file 559
Figure 192: Example telnet session to clear custom files 560
Figure 193: Protocol analysis at the SM 561
Figure 194: Protocol analyzer at AP not connected to a CMM 562
Figure 195: Protocol analysis at AP connected to a CMM 563
Figure 196: Local Area Connection Properties window 564
Figure 197: Internet Protocol (TCP/IP) Properties window 565
Figure 198: Wireshark Capture Options window 566
Figure 199: Wireshark Capture window 567
Figure 200: <capture> - Wireshark window, Packet 1 selected 568
Figure 201: <capture> - Wireshark window, Packet 14 selected 569

List of Tables

Table 1: User guide organization scheme 25
Table 2: Examples of where to find information in this user guide 26
Table 3: Font types 28
Table 4: Admonition types 29
Table 5: Essential user guide elements for new wireless Ethernet bridge network implementation 33
Table 6: Fixed wireless broadband IP network product names 35
Table 7: Power supply descriptions 54
Table 8: Line Cords for Power Supplies 55
Table 9: Recommended outdoor UTP Category 5E cables 58
Table 10: Recommended indoor UTP Category 5E cables 58
Table 11: Recommended antenna cables 59
Table 12: Product applications per frequency band range 61
Table 13: Products with encryption options available per frequency band, PMP links 62
Table 14: Typical range and throughput per frequency band, PMP links 63
Table 15: Typical range and throughput per frequency band, PTP links 65
Table 16: Cluster management product similarities and differences 66
Table 17: Applications and tools 69
Table 18: Correct placement of license keys 74
Table 19: Model numbers 79
Table 20: Labels and locations of model (part) numbers and ESNs 80
Table 21: Characteristics of traffic scheduling 88
Table 22: Effect of 2X operation on throughput for the SM 90
Table 23: OFDM module performance at 1X, 2X, and 3X operation 93
Table 24: Effects of network conditions on PTMP throughput 100
Table 25: Comparison of SM products with CAP 130 100
Table 26: List of features 104
Table 27: Demonstration Kit part numbers 119
Table 28: Starter Kit part numbers 122
Table 29: Effect of DFS feature 128
Table 30: United States Region Code – unavailble center channels 130
Table 31: Signal quality levels indicated by jitter 132
Table 32: Recommended courses of action based on Efficiency in 2X operation 133
Table 33: Available center channels for single OFDM AP 138
Table 34: Example 900-MHz channel assignment by sector 140
Table 35: Example 2.4-GHz channel assignment by sector 141
Table 36: Example 5.2-GHz channel assignment by sector 141
Table 37: Example 5.4-GHz channel assignment by sector 141
Table 38: Example 5.7-GHz FSK channel assignment by sector 142

Table 39: Example 5.8-GHz OFDM channel assignment by sector, 5 MHz guard band between adjacent sectors.143
Table 40: Example 5.8-GHz OFDM channel assignment by sector, 5 MHz guard band between adjacent sectors.144
Table 41: VLAN filters in point-to-multipoint modules.168
Table 42: Q-in-Q Ethernet frame.169
Table 43: Exposure separation distances.174
Table 44: Calculated exposure distances and power compliance margins.176
Table 45: Statistical incidence of current from lightning strikes.178
Table 46: LEDs in AP and BHM.185
Table 47: Legacy Mode LEDs in SM and BHS.186
Table 48: Revised Mode LEDs in SM.186
Table 49: Control slot settings for all FSK APs in cluster.251
Table 50: Control slot settings for all OFDM APs in cluster.251
Table 51: Recommended External Gain values for AP.254
Table 52: Broadcast Downlink CIR achievable per Broadcast Repeat Count.260
Table 53: Recommended combined settings for typical operations.325
Table 54: Where feature values are obtained for an SM with authentication required.326
Table 55: Where feature values are obtained for an SM with authentication disabled.326
Table 56: Recommended External Gain values for AP.338
Table 57: Recommended External Antenna Gain values for BHS.365
Table 58: Total gain per antenna.383
Table 59: Patch antenna and reflector gain.383
Table 60: Transmitter output power settings, example cases.384
Table 61: Hardware series by MAC address.425
Table 62: Hardware series differences.425
Table 63: Ports filtered per protocol selections.437
Table 64: Example times to download for typical tiers of service with CAP 120.441
Table 65: Example times to download for typical tiers of service with CAP 130.442
Table 66 RADIUS Vendor Specific Attributes (VSAs).452
Table 67: AP User Authentication attributes.456
Table 68: SM User Authentication attributes.457
Table 69: SNMP Proxy flow.461
Table 69: Categories of MIB-II objects.465
Table 70: Canopy Enterprise MIB objects for APs, SMs, and BHs.467
Table 71: Canopy Enterprise MIB objects for APs and BH timing masters.481
Table 72: Canopy Enterprise MIB objects for SMs and BH timing slaves.488
Table 73: Event Log messages for abnormal events.505
Table 74: Event Log messages for normal events.506
Table 75: Ethernet tab attributes.512
Table 76: RF Control Block statistics attributes.514
Table 77: Data VC attributes.517
Table 77: Overload tab attributes.519
Table 77: DHCP Relay attributes.521
Table 78 NAT Stats attributes.523

Table 79: Supported telnet commands for module administration 581
Table 80: US FCC IDs and Industry Canada certification numbers and covered configurations.....584
Table 81: Disclosure Table for China.....592

Chapter 1: About this User Guide

Purpose

Cambium Networks Point-To-Multipoint (PMP) documents are intended to instruct and assist personnel in the operation, installation and maintenance of the Cambium PMP equipment and ancillary devices. It is recommended that all personnel engaged in such activities be properly trained.

Cambium disclaims all liability whatsoever, implied or express, for any risk of damage, loss or reduction in system performance arising directly or indirectly out of the failure of the customer, or anyone acting on the customer's behalf, to abide by the instructions, system parameters, or recommendations made in this document.

Cross references

References to external publications are shown in italics. Other cross references, emphasized in blue text in electronic versions, are active links to the references.

This document is divided into numbered chapters that are divided into sections. Sections are not numbered, but are individually named at the top of each page, and are listed in the table of contents.

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. Send feedback to email support (see ‘Contacting Cambium Networks’).

Problems and warranty

Reporting problems

If any problems are encountered when installing or operating this equipment, follow this procedure to investigate and report:

1. Search this document and the software release notes of supported releases.
2. Visit the support website. http://www.cambiumnetworks.com/support/pmp/software/index.php
3. Ask for assistance from the Cambium product supplier.
4. Gather information from affected units such as:
   - The IP addresses and MAC addresses.
   - The software releases.
   - The configuration of software features.
   - Any available diagnostic downloads.
   - CNUT Support Capture Tool information
5. Escalate the problem by emailing or telephoning support.

See ‘Contacting Cambium Networks’ for URLs, email addresses and telephone numbers.

Repair and service

If unit failure is suspected, obtain details of the Return Material Authorization (RMA) process from the support website.

Warranty

Cambium’s standard hardware warranty is for one (1) year from date of shipment from Cambium or a Cambium distributor. Cambium warrants that hardware will conform to the relevant published specifications and will be free from material defects in material and workmanship under normal use and service. Cambium shall within this time, at its own option, either repair or replace the defective product within thirty (30) days of receipt of the defective product. Repaired or replaced product will be subject to the original warranty period but not less than thirty (30) days.

To register PMP products or activate warranties, visit the support website.

Extended warranties are available for PMP products. For warranty assistance, contact the reseller or distributor.

Using non-Cambium parts for repair could damage the equipment or void warranty. Contact Cambium for service and repair instructions.

Portions of Cambium equipment may be damaged from exposure to electrostatic discharge. Use precautions to prevent damage.

Security advice

Cambium Networks systems and equipment provide security parameters that can be configured by the operator based on their particular operating environment. Cambium recommends setting and using these parameters following industry recognized security practices. Security aspects to be considered are protecting the confidentiality, integrity, and availability of information and assets. Assets include the ability to communicate, information about the nature of the communications, and information about the parties involved.

In certain instances Cambium makes specific recommendations regarding security practices, however the implementation of these recommendations and final responsibility for the security of the system lies with the operator of the system.

Portfolio of Wireless Broadband Solutions

The Cambium portfolio of wireless broadband solutions provides a range of flexible options including

- Fixed
  - unlicensed point-to-multipoint solutions
  - Expedience licensed point-to-multipoint solutions
  - point-to-point solutions
- WiMAX, including infrastructure, CPE and devices, services

Products Covered by This User Guide

Products covered by this user guide include

- PMP 100 Series FSK Access Points (CAPs) and Subscriber Modules (CSMs) in the following frequency bands:
  - 900 MHz
  - 2.4 GHz
  - 5.2 GHz
  - 5.4 GHz
  - 5.7 GHz
- PMP 400 Series OFDM Access Points (CAPs) and Subscriber Modules (CSMs) in the following frequency bands:
  - 4.9 GHz
  - 5.4 GHz
- PTP 100 Series FSK bridges in the following frequency bands:
  - 2.4 GHz
  - 5.2 GHz
  - 5.8 GHz

- 5.1 GHz
- 5.4 GHz

- PTP 200 Series OFDM bridges in the following frequency bands:
  - 4.9 GHz
  - 5.4 GHz
- 600SS Surge Suppressor

Products Not Covered by This User Guide

Products with their own user guides include

- PTP 250, 300, 400, 500, 600, 800, 810/810i Series Bridges
- PMP 430, 450 / PTP 200,230 Series Networks
- PMP 320 Series Networks
- Cluster Management Module 2 (CMM2)
- Cluster Management Module micro (CMMmicro or CMM3)
- Cluster Management Module 4 (CMM4)
- Prizm element management system
- Wireless Manager network management system

All of these products and solutions are covered by their own user guides and/or other documentation.

Software Compatibility Described in This User Guide

The following sections of this document provide details and caveats about the compatibility of products:

- Designations for Hardware on Page 425
- MIB File Set Compatibility on Page 426

Chapter 2: Using This User Guide

This document should be used with features in Software Release 11.2. The audience for this document includes system operators, network administrators, and equipment installers.

Finding the Information You Need

Becoming Familiar with This User Guide

This is a guide to the guide. A high-level overview of the guide and some examples of where to look provide insight into how information is arranged and labeled.

The Table of Contents provides not only a sequential index of topics but also a visual glance at the organization of topics in this guide. A few minutes spent with the Table of Contents in either the paper or the electronic version of this guide can save much more time in finding information now and in the future. The List of Procedures may be especially useful in the paper version of this guide, particularly where you mark those procedures that you wish to frequently see.

In contrast, the List of Figures and List of Tables are most useful for automated searches on key words in the electronic version of this guide. If a match is present, the match is the first instance that the search finds.

Quick Reference

This user guide comprises six sections, as described in Table 1.

Table 1: User guide organization scheme

Section	Purpose
Guide to This User Guide (this section)	Identifies ◦ products covered by this user guide. ◦ products covered by their own separate user guides. ◦ how this user guide is organized. ◦ where to find module web pages and parameter descriptions. ◦ what the various typefaces and admonitions indicate. ◦ how to contact Cambium.

Section	Purpose
Overview of Fixed Wireless Broadband IP Networks	Provides ◦ references to RF and networking theory. ◦ a list of sections to see if you are building only a backhaul network. ◦ overviews and comparisons of products and how they communicate. ◦ descriptions of data handling and synchronization. ◦ a review of optional features. ◦ resources for developing familiarity and proficiencies with networks.
Planning Guide	Provides essential information for ◦ evaluating an area for a network. ◦ specifying the IP addresses and frequency band ranges to use for each type of link.
Installation and Configuration Guide	Provides systematic approaches for ◦ avoiding hazards from RF and natural causes. ◦ testing, storing, and deploying equipment.
Operations Guide	Provides guidance for ◦ expanding network coverage. ◦ improving the security of wireless links. ◦ distributing bandwidth resources. ◦ monitoring and changing variables through SNMP.
Reference Information	Provides supplemental information such as ◦ authorizations, approvals, and notices. ◦ a bibliography of adjunctive information sources. ◦ a history of changes in documentation.
Glossary	Defines terms and concepts that are used in this user guide.

Examples

A list of common tasks and references to information that supports each task is provided in Table 2.

Table 2: Examples of where to find information in this user guide

If you want to know…	then see…	because…
what the Spectrum Analyzer in SM and BHS feature does	Avoiding Self Interference on Page 154	this topic is important to RF planning.
	Monitoring the RF Environment on Page 420	this topic is also important to managing the network.
what types of slots compose the frame	Understanding Bandwidth Management on Page 81	this information is helpful for understanding networks.

If you want to know…	then see…	because…
how to calculate whether an object will interfere with a signal	A reflected signal can arrive at the antenna of the receiver later than the non-reflected signal arrives. These two or more signals cause the condition known as multipath. Multipath may increase or decrease the signal level and so overall attenuation may be higher or lower than that caused by the link distance. This is problematic at the margin of the link budget, where the standard operating margin (fade margin) may be compromised. Noting Possible Obstructions in the Fresnel Zone on Page 126	this topic is important to RF planning.
how long a cable you can use from the GPS antenna to the CMM	Cables on Page 25	cables are accessory components.
	the dedicated user guide that supports the CMM that you are deploying.	the advisory applies to mounting GPS antennas *and* CMMs.
how to react to a WatchDog Event Log message	Messages that Flag Abnormal Events on Page 505 *and* Messages that Flag Normal Events on Page 506	together, these two sections document all significant Event Log messages.
what beam angle the passive reflector dish produces	Specifications and Limitations on Page 74, then downward to a table for a part number that includes “RF.”	the beam angle is a specification.
how to aim the passive reflector dish	Installing a Reflector Dish on Page 408	aiming is associated with installation of wireless bridges.
how to set Differentiated Services values so that traffic with original ToS byte formatting continues to be prioritized as it was before DSCP fields.	High-priority Bandwidth on Page 86	DSCP fields specify the level of priority that the device is requesting for the packet.

Searching This User Guide

To search this document and the software release notes of supported releases, look in the Table of Contents for the topic and in the Adobe Reader® search capability for keywords that apply.[1] These searches are most effective when you begin the search from the cover page because the first matches may be in titles of sections, figures, tables, or procedures.

Interpreting Typeface and Other Conventions

This document employs distinctive fonts to indicate the type of information, as described in Table 3.

Table 3: Font types

Font	Type of Information
variable width bold	Selectable option in a graphical user interface or settable parameter in the web-based interface to a component.
`constant width regular`	Literal system response in a command-line interface.
`constant width italic`	Variable system response in a command-line interface.
`constant width bold`	Literal user input in a command-line interface.
`constant width bold italic`	Variable user input in a command-line interface.

This document employs specific imperative terminology as follows:

- *Type* means press the following characters.
- *Enter* means type the following characters and then press Enter.

[1] Reader is a registered trademark of Adobe Systems, Incorporated.

This document also employs a set of consistently used admonitions. Each of these types of admonitions has a general purpose that underlies the specific information in the box. These purposes are indicated in Table 4.

Table 4: Admonition types

Admonition Label	General Message
	NOTE: informative content that may ◦ defy common or cursory logic. ◦ describe a peculiarity of the implementation. ◦ add a conditional caveat. ◦ provide a reference. ◦ explain the reason for a preceding statement or provide prerequisite background for what immediately follows.
	RECOMMENDATION: suggestion for an easier, quicker, or safer action or practice.
	IMPORTANT! informative content that may ◦ identify an indication that you should watch for. ◦ advise that your action can disturb something that you may not want disturbed. ◦ reiterate something that you presumably know but should always remember.
	CAUTION! a notice that the risk of harm to equipment or service exists.
	WARNING! a notice that the risk of harm to person exists.

Sending Feedback

Is this document accurate, complete, and clear? How can it be improved? Send your feedback on documentation to support@cambiumnetworks.com.

Overview of PMP Solutions

Chapter 3: Advancing from Research to Implementation

Before you begin to research a possible implementation, you should have both

- basic knowledge of RF theory. See
  - Understanding RF Fundamentals on Page 115.
  - Engineering Your RF Communications on Page 123.
- network experience. See
  - Link Characteristics on Page 81.
  - Understanding IP Fundamentals on Page 115.
  - Engineering Your IP Communications on Page 157.

Chapter 4: Realizing a Wireless Ethernet Bridge Network

PTP 100 Series Bridges serving as backhaul modules (BHs) can connect access point clusters to the point of presence or be the backbone of a Metro WiFi mesh network. In other applications, the backhaul modules can be used to provide connectivity for

- cell sites, in lieu of leased T1/E1 telecommunications lines.
- buildings in corporate or institutional campuses.
- remote sites, including temporary sites set up for relief efforts.

These BHs are available in 10- or 20-Mbps modulation rates from the factory. The rate is distinguished as BH10 or BH20 in the Software Version field of the General Status tab (in the Home page) of the module GUI.

For these and any other backhaul networks, Table 5 provides a quick reference to information that you would need to establish and maintain the wireless bridge network.

Table 5: Essential user guide elements for new wireless Ethernet bridge network implementation

Title	Page
Products Not Covered by This User Guide	24
PTP Series 100 Bridges	40
PTP 200 Series Bridges	41
PTP 400 Series Bridges	41
PTP 500 Series Bridges	42
PTP 600 Series Bridges	42
Cluster Management Module-2 (Part 1008CK-2)	47
Cluster Management Module micro (Part 1070CK)	47
CMM4 (Part 1090CK, 1091AA)	49
Typical range and throughput per frequency band, PTP links	65
BH-BH Links	99
Typical multiple-BH network layout	103
Analyzing the RF Environment	124
Considering Frequency Band	134
Avoiding Hazards	174

Configuring a Point-to-Point Link for Test	218
Preparing Components for Deployment	234
Configuring a BH Timing Master for the Destination	327
Configuring a BH Timing Slave for the Destination	355
Installing a GPS Antenna	395
Installing a	395
Installing a Reflector Dish	408
Installing a BH Timing Master	410
Installing a BH Timing Slave	412
Verifying a BH Link	415
Encrypting Radio Transmissions	428
Managing Module Access	430
Objects Defined in the Canopy Enterprise MIB	467
Interface Designations in SNMP	496
Traps Provided in the Canopy Enterprise MIB	497
Using the Canopy Network Updater Tool (CNUT)	499
Typical Contents of Release Notes	555
Typical Upgrade Process	555
Analyzing traffic at an AP or BH with no CMM	562
Analyzing Traffic at an AP or BH with a CMM	562
Troubleshooting	570

Chapter 5: Exploring the Scope of Solutions

Fixed wireless broadband IP network applications include:

- local area network (LAN) extensions
- Internet subscriber service
- high-bandwidth point-to-point connections
- multicast video (for instruction or training, for example)
- private branch exchange (PBX) extensions
- point-to-multipoint data backhaul
- redundant network backup
- video surveillance
- voice over IP (VoIP)
- TDM over Ethernet (for legacy voice and data)

Product Names

Table 6 defines the network product names of devices covered in this user guide.

Table 6: Fixed wireless broadband IP network product names

Protocol Type	Product Series	Product Name	Previous Names	Example Model
Point-to-Multipoint	PMP 100	CAP 120	CAP 100, Classic AP	5700AP
		CSM 120	CSM 100, SM	5700SM
		CSM 110	Lite SM	5760SM
		CAP 130	CAP 200, Advantage AP	5750AP
		CSM 130	CSM 200, Advantage SM	5750SM
	PMP 400	CAP 49400	4.9-GHz OFDM AP	4940AP
		CSM 49400	4.9-GHz OFDM SM	4940SM
		CAP 54400	5.4-GHz OFDM AP	5440AP
		CSM 54400	5.4-GHz OFDM SM	5440SM
Point-to-Point	PTP 100	PTP 110	2- or 4-Mbps BH	
		PTP 120	PTP 100 Lite, BH10 (7-Mbps)	5700BH

Protocol Type	Product Series	Product Name	Previous Names	Example Model
		PTP 130	PTP 100 Full, BH20 (14-Mbps)	5700BH20
	PTP 200	PTP 49200	4.9-GHz OFDM BH	4940BH
		PTP 54200	5.4-GHz OFDM BH	5440BH

NOTE:

Each product is available in multiple model numbers, which distinguish the model by such attributes as frequency band range, encryption type, or power adjustable for extended range. See Interpreting Model Number on Page 76 and Sorted Model Numbers on Page 78.

Network Components

Cambium fixed wireless broadband IP networks use some or all of the following components. For the components that provide a graphical user interface (GUI), access to the GUI is through a web browser. In Release 8 and later, cascading style sheets (CSS) configure the GUI. Thus an operator is able to customize the GUI by editing these style sheets.

Access Point Module Other Than 900-Mhz

The FSK Access Point (AP) module provides up to 14 Mbps aggregate throughput in a 60° sector. The CAP 120 FSK AP can communicate with only a CSM 120 SM, *not also* a CSM 130 or a Lite (CSM 110) SM. The CAP 130 or CAP 09130 AP distributes services as broadly as the CAP 120. However, the CAP 130 provides greater throughput and less latency. The CAP 130 communicates with all SMs in its frequency band range: CSM 110s, CSM 120s, and CSM 130s.

The OFDM AP provides up to 21 Mbps aggregate throughput in a 90° sector. An OFDM AP can communicate with only an OFDM SM.

An FSK or OFDM AP supports up to 200 subscribers and 4,096 MAC addresses, which may be directly-connected PCs, IP appliances, gateways, Subscriber Modules (SMs), and the AP, except that *no limit* applies behind subscriber network address translation (NAT) gateways. The AP is configurable through a web interface.

Access Point Cluster

An AP cluster covers as much as 360°.

The FSK (PMP 100 or PMP 400) AP cluster consists of two to six APs that together provide broadband connectivity to 1,200 or fewer subscribers. Each of these APs transmits and receives in a 60° sector.

The PMP 400 Series (OFDM) AP cluster consists of two to four APs that provide broadband connectivity to 800 or fewer subscribers. Each of these APs transmits and receives in a 90° sector.

An AP cluster is pictured in Figure 1.

Figure 1: Pole-mounted AP cluster

The variety of available FSK and OFDM APs in frequency band range, power adjustability, and antenna configuration is shown under Acquiring a Demonstration Kit, beginning on Page 115.

An OFDM AP, showing the antenna in front and the radio attached to it, is pictured in Figure 2.

Figure 2: OFDM AP - Antenna and Radio

Subscriber Module Other Than 900-MHz

The Subscriber Module (SM) is a customer premises equipment (CPE) device that provides broadband services through communication with an AP. The SM is configurable through a web interface.

The variety of available FSK and OFDM SMs in frequency band range, power adjustability, and antenna configuration is shown under Acquiring a Demonstration Kit, beginning on Page 115.

Figure 3: Structure-mounted SM

The CSM 130 or CSM 09130 provides the same configurability and services as the CSM 110 or CSM 120. However, in a link with a CAP 130 or CAP 09130, the CSM 130 or CSM 09130 provides uncapped sustained 2X throughput. See 2X Operation on Page 89. A CSM 130 or CSM 09130 can communicate with only a CAP 130 or CAP 09130, respectively.

A PMP 100 Series (FSK SM) can communicate with either a CAP 120 or CAP 130. An FSK SM mounted directly to a structure is pictured in Figure 3.

A PMP Series 400 (OFDM) SM can communicate with only an OFDM AP. An OFDM SM is shown in Figure 4 in both front and side views.

Figure 4: OFDM SM, front and side views

Lite SMs (CSM 110 modules) cost less and provide less throughput than the CSM 120s or CSM 130s. They support the same radio frequencies, interference tolerance, and product reliability. They give operators the additional option to serve cost-sensitive customers who want standard services (web browsing, email, VoIP, and downloads), but do not require the higher throughput that is available with a regular SM. Lite SMs support an aggregate (uplink plus downlink) throughput of 512 kbps.

Through purchased floating licenses that Prizm manages, they are upgradeable to 1, 2, 4, or 7 Mbps aggregate throughput. A Lite SM can communicate with only a CAP 130. A comparison of the CSM 110 to the CSM 120 and CSM 130 is provided in Table 25 on Page 100.

900-MHz AP and SM

The 900 MHz AP (CAP 09130) and SM (CSM 09130) modules operate at a 3.3 Mbps carrier rate (compared to 10 Mbps for other FSK frequency bands).

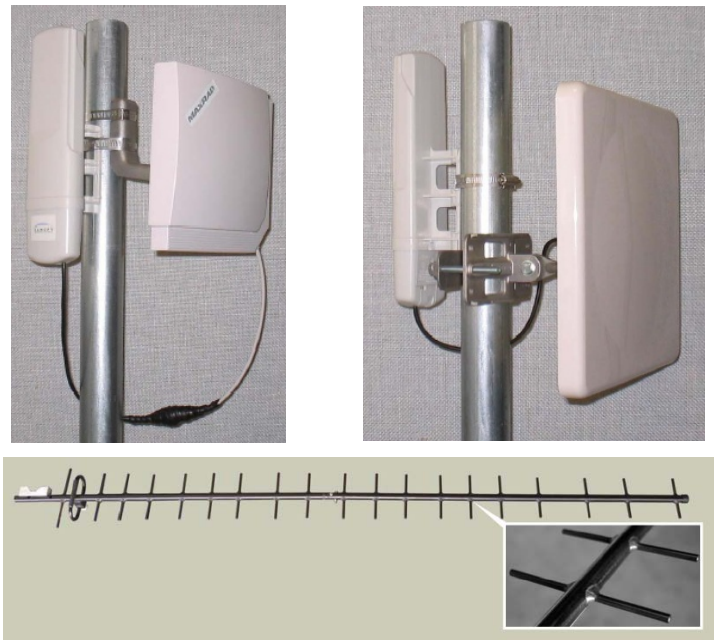


Figure 5: Examples of antennas for 900-MHz modules

These 900-MHz modules run the same software and provide the same parameters, network features, and connections as all other APs and SMs. The physics of longer-wavelength 900 MHz, the power allowed by regulatory authorities, and the low required level of Carrier-to-Interference (C/I) ratio combine to support

- line of sight (LOS) range of up to 40 miles (over 64 km)

increased non-line of sight (NLOS) range, depending on RF considerations such as foliage, topography, and obstructions.

When co-located with an SM of another frequency band range, the 900-MHz AP may serve, without a tower or BH, as a *remote* AP (see Deploying a Remote AP on Page 150). 900-MHz AP/SM links are logical choices for extending radio networks where you wish to

- add subscriber-handling capacity to a tower that is either
  - fully used in the other frequency band ranges.
  - not available to any other frequency band range.
- reach sparsely populated areas.
- penetrate foliage.
- add a remote AP behind an SM that operates in another frequency band range.

With Only the Integrated Antenna

The enclosure of the 900-MHz integrated AP and SM houses both the hardware and antenna. These modules can be purchased with a band pass filter to improve performance in environments in which equipment (for example, a pager) is operating in the spectrum adjacent to the 900-MHz band.

Unlike the antennas in other FSK Cambium radios, the integrated antenna in the 900-MHz radio is *horizontally* polarized to reduce exposure to noise from vertically polarized signals, which predominate in this band.

Connectorized for External Antenna

The enclosure of the 900-MHz connectorized AP and SM includes a cable and N-type connector to which an external antenna can attach. In this case, network operators can select horizontal or vertical polarization and select the type of antenna to use. However, these connectorized modules can be used in the same architecture with the integrated modules only if the connectorized modules are *horizontally* polarized.

PTP Series 100 Bridges

A pair of PTP 100 Series wireless Ethernet bridges provides point-to-point connectivity as either a standalone link or a link through a cluster management module to an AP cluster.

You must configure a BH as either a timing master (BHM) or timing slave (BHS). The BHM provides synchronization signal (sync) to the BHS.

A BH mounted to a passive reflector dish is pictured in Figure 6. Carrier applications for these modules include reaching remote AP clusters, interconnecting campus buildings or remote branch offices, extending private branch exchange (PBX) circuits, backhauling cell sites, and extending central office T1s/E1s.

These BHs are supported by this user guide. See Realizing a Wireless Ethernet Bridge Network on Page 33.

Figure 6: Dish-mounted 7.5- or 14-Mbps bridge

PTP 200 Series Bridges

The PTP 200 Series bridges securely transport data, voice, and video in both near-line-of-sight (nLOS) and line-of-sight (LOS) deployments at Ethernet data rates up to 21 Mbps. In the 4.9-GHz range, the public safety area of the spectrum, these bridges are a point-to-point solution for emergency services. In 5.4 GHz, they are a solution for enterprises. Orthogonal Frequency Division Multiplexing (OFDM) technology resists multi-path interference and fading that is otherwise caused by buildings and other obstructions.

Figure 7: 21-Mbps bridge

Interference avoidance capability is ensured. The Dynamic Frequency Selection (DFS) feature switches channels to avoid interfering with priority signals. Moreover, these bridges can be co-located within the physical scope of an existing network, or used as part of a 5.4-GHz frequency band overlay network.

These bridges are supported by this user guide. See Realizing a Wireless Ethernet Bridge Network on Page 33.

PTP 300 Series Bridges

PTP 300 Series wireless Ethernet bridges offer reliable and cost-effective backhaul at rates up to 25 Mbps for distances up to 155 miles (250 km) or, when enabled by a special license key, up to 50 Mbps in LOS deployments for distances up to 10 miles (16 km).

These bridges operate in the 5.4- or 5.8-GHz frequency band range. The form for these bridges is shown in Figure 8. These bridges are supported by their own dedicated user guide.

PTP 400 Series Bridges

PTP 400 Series wireless Ethernet bridges offer reliable non-line-of-sight (NLoS) or long-distance line of sight (LoS) connection to the other bridge in the pair. Their features include adaptive modulation, intelligent Dynamic Frequency Selection, and a preset that denies connection to any unit other than the one in its pair. These are available as full (43-Mbps) or lite (21-Mbps) bridges.

Figure 8: PTP 300/400/500/600 Series Bridge common form

Either variety is a solution for any of the following field applications:

- backhaul pair for PMP networks
- campus connection between buildings

- last-mile access and backbone
- voice over IP (VoIP) and video surveillance

These bridges transmit and receive in the 4.9-GHz frequency band range, at 4.940 to 4.990. The form for these bridges is shown in Figure 8. These bridges are supported by their own dedicated user guide.

PTP 500 Series Bridges

Cambium PTP 500 Series Bridges offer reliable non-line-of-sight (NLoS) and long-distance line of sight (LoS) connection to the other bridge in the pair. Their features include Multiple-input Multiple-output (MIMO), intelligent Orthogonal Frequency Division Multiplexing (i-OFDM), Advanced Spectrum Management, and Adaptive Modulation. These are available as 105-Mbps bridges. These bridges transmit and receive in 5.4- and 5.8-GHz frequency band ranges. The form for these bridges is shown in Figure 8 on Page 41.

They are a solution for any of the following field applications:

- high-speed backhaul
- campus connection between buildings
- telemedicine
- disaster recovery
- emergency services
- voice over IP (VoIP) and video surveillance

The PTP 500 Series Bridges offer many more SNMP-accessible element management parameters than do their PTP 400 and 600 Series counterparts; specifically, a significantly larger number of read-only fields, manageable objects, and notifications addressable to the NMS. Further, a new PTP LINKPlanner tool currently supports only PTP 500 Bridge networks. This tool allows operators to simultaneously see path calculations for configuring single and multiple links, using a Google Earth overview. In this way, the PTP LINKPlanner can be more useful than the Link Estimator tool, which continues to support the PTP 400 and 600 Series wireless bridges that Cambium offers.

These bridges are supported by their own dedicated user guide.

PTP 600 Series Bridges

Cambium PTP 600 Series Bridges offer reliable non-line-of-sight (NLoS) and long-distance line of sight (LoS) connection to the other bridge in the pair. Their features include adaptive modulation, intelligent Dynamic Frequency Selection, and a preset that denies connection to any unit other than the one in its pair. These are available as full (300-Mbps) or lite (150-Mbps) bridges.

Each pair of these bridges transmits and receives in one of the following frequency band ranges. The bridges manufactured for

- the 2.5-GHz range, which is the Educational Broadcast Service area of the spectrum, constitute a PTP solution for low-power high-speed distance learning with Internet access and email in any of the following field applications:
  - backhaul pair for PMP networks
  - campus connection between buildings
  - last-mile access and backbone
  - voice over IP (VoIP) and video surveillance
- the 4.5- and 4.8-GHz ranges, which together are the U.S. government and military and the NATO areas of the spectrum, constitute PTP solutions for
  - battlefield communications
  - campus connection between buildings
  - training and simulation networks
  - video surveillance and border security
- the 4.9-GHz range, which is the public safety area of the spectrum, constitute PTP solutions for
  - missing-person, DMV, and medical records
  - building blueprints and vehicle locations
  - primary, secondary, and infill, ASTRO links
  - part of a pre-mounted emergency site
- the 5.4-, 5.8-, and 5.9-GHz ranges constitute PTP solutions for unlicensed backhaul of bundled circuit-switched VoIP, video, and data communications.

The form for these bridges is shown in Figure 8 on Page 41. These bridges are supported by their own dedicated user guide.

PTP 800 Series Bridges

Today's converged multi-service networks need high capacity, availability, reliability and security with low latency and true affordability. Our Cambium PTP 800 Licensed Ethernet portfolio has been designed to ensure that today's evolving networks can benefit from the highest level of IP-optimized microwave solutions available in the market. For public safety agencies, government entities, enterprises and service providers who demand licensed exclusivity, high-bandwidth, scalability and affordability, the PTP 800 Series can meet all of your network and bandwidth requirements.

Because our portfolio supports both Split Mount and All-Indoor architectures, network operators can choose a solution that best accommodates their unique business needs. Whether providing connectivity to long distance locations, backhauling video or providing last-mile access, the PTP 800 and PTP 800i All-Indoor solutions have the capabilities and features to meet today's IP requirements and tomorrow's Next Generation Network needs.

Today's converged multi-service networks need high capacity, availability, reliability and security with low latency and true affordability. Our Cambium PTP 800 Licensed Ethernet portfolio has been designed to ensure that today's evolving networks can benefit from the highest level of IP-optimized microwave solutions available in the market. For public safety agencies, government entities, enterprises and service providers who demand licensed exclusivity, high-bandwidth, scalability and affordability, the PTP 800 Series can meet all of your network and bandwidth requirements.

Because our portfolio supports both Split Mount and All-Indoor architectures, network operators can choose a solution that best accommodates their unique business needs. Whether providing connectivity to long distance locations, backhauling video or providing last-mile access, the PTP 800 and PTP 800i All-Indoor solutions have the capabilities and features to meet today's IP requirements and tomorrow's Next Generation Network needs.

Operating in the 6 to 38 GHz RF bands* at up to 368 Mbps throughput (full duplex) and with user-configured channel bandwidths from 7 to 56 MHz, the Cambium PTP 800 Series offers operators a highly reliable licensed band solution. With upgradeable capacity from 10 Mbps to full capacity via a software key, the systems offer exceptional cost efficiency and scalability. The PTP 800i All-Indoor system delivers up to 236 Mbps (full duplex) over configurable channel bandwidths from 10 to 40 MHz. In addition, Cambium offers comprehensive FCC licensing coordination services through our partnership with Comsearch.

Key features include:

- 1+1: Includes 1+1 Hot Standby links, 2+0 redundant links in a ring or mesh configuration plus non-redundant links. Hot Standby links are designed to provide full redundancy in the event of a single Compact Modem Unit (CMU) or an Outdoor Unit (ODU) failure at one or both ends of the link.

- Effective system design: With the smallest Compact Modem Unit (CMU) in the industry, the small form factor design helps remove customer dependency on rack space.

- Capacity as you grow throughput: Flexible stepping options allow operators to purchase a standard 10 Mbps factory set cap and then increase capacity as needed based on throughput demands ensuring exceptional scalability.

- Asymmetric control: Where users download more information than they upload, operators can assign different throughput capacities for the up and down links.

- No surprises link planning: Optimize licensed link performance prior to purchase and gain a complete view of your network via Google Earth with the PTP LINKPlanner. This tool also provides a complete Bill of Materials (BOM) that lists all equipment required for the deployment simplifying the order process and providing important link information needed for FCC and other regulatory bodies.

- Security Options: FIPS-197 128/256-bit AES encryption, FIPS 140-2

- Low Latency: < 115us @ full capacity with 64 bytes

- Flexible network management: Remote management via web browser. Optional Cambium Wireless Manager or other third party tools are available for management purposes.

  "Zero-Downtime" Adaptive Modulation: Automatic shifting of modulation and/or coding rate as radio path conditions change enable transmitters and receivers to negotiate highest mutually sustainable data rate.

PTP 810/810i Series Bridges

Cambium Networks carrier-grade PTP 810 licensed microwave solutions provide reliable, high-capacity connectivity and backhaul for both your Ethernet and TDM applications. The systems operate in radio frequencies between 6 and 38 GHz at scalable Ethernet data rates up to 700 Mbps full duplex. The modular design offers pluggable modem units that support T1/E1, STM-1, and Ethernet on a single platform; giving you great flexibility to configure the best system for your needs at the optimal cost. The systems are available in both Split Mount and All-Indoor (PTP 810i) architectures. PTP 810i All-Indoor solutions provide an optimal solution when tower access is difficult whether due to weather or other inaccessibility. Available in FCC and ICC 6 and 11 GHz authorized bands, these fixed licensed solutions can obtain up to 477 Mbps with XPIC enabled.

The demands to support more multimedia communications, mobility, and deliver higher throughputs for bandwidth intensive applications is growing exponentially. Now operators can leverage their legacy investment while taking advantage of the cost efficiencies and performance benefits of packet-based Ethernet technology. Service providers, public safety and government agencies, heavy industry such as utilities and transportation and other enterprises will find PTP 810 an optimal solution for making this migration. Capital expenditures and operating expenses can be reduced to support a number of applications including:

- Lease line Replacement
- Network Redundancy
- Video Surveillance Backhaul
- Building to Building and Campus Connectivity
- Wireless Network Extensions

The PTP 810 includes:

- Modular Modem Unit Design — Supports T1/E1, STM-1, and Ethernet on a single platform offering flexibility for your unique configuration requirements
- XPIC – This functionality allows you to double throughput capacity without increasing channel bandwidth by transmitting different data on both the horizontal and vertical polarizations in the same channel
- Link Aggregation — Supports true link aggregation over a single link while most comparative systems require two ports to get similar throughput
- Robust Capacity – Highly scalable throughput up to 700 Mbps full duplex with XPIC
- Configurable Channel Widths – 7 to 80 MHz
- Built In Cross Point Switch – Enables channel mapping without the addition of more equipment
- Multiple System Configurations – Supports 1+0 Non-Protected, 1+1 Protected, 1+1 Protected w/Spatial Diversity, 1+1 w/Frequency Diversity, 2+0 for Link Aggregation, 2+0 Ring, Protected PDH Ring, SNCP-Like Protected T1/E1, Protected Ethernet Ring
- Enhanced QoS – Protects your voice and high priority traffic

Radio Adjustable Power Capabilities

Cambium offers adjustable power radios in all frequency bands. See Adjusting Transmitter Output Power on Page 382 to ensure that your radios do not exceed the maximum permitted EIRP.

Cluster Management Module-2 (Part 1008CK-2)

The Cluster Management Module-2 (CMM2) provides power, GPS timing from an antenna that is included, and networking connections for an AP cluster. The CMM2 can also connect to a BH, in which case the CMM2 is the central point of connectivity for the entire site. The CMM2 can connect as many as eight co-located modules—APs, BHMs, BHSs—and an Ethernet feed.

The CMM2 requires two cables for each connected module:

- One provides Ethernet communications and power. This cable terminates in an RJ-45 connector.
- The other provides synchronization (sync), GPS status, and time and date in a serial interface. This cable terminates in an RJ-11 connector.

A CMM2 is pictured in Figure 9. A CMM2 as part of a mounted system is pictured in Figure 10. CMM2 is no longer available for purchase, but it still a supported product. For documentation, it is supported by its own dedicated user guide.

Figure 9: CMM2 enclosure

Figure 10: CMM2 pole-mounted

Cluster Management Module micro (Part 1070CK)

The Cluster Management Module micro (CMMmicro) provides power, GPS timing, and networking connections for an AP cluster. The CMMmicro is configurable through a web interface.

The CMMmicro contains an 8-port managed switch that supports Power over Ethernet (PoE) on each port and connects any combination of APs, BHMs, BHSs, or Ethernet feed. The Cambium fixed wireless broadband IP networks PoE *differs from* IEEE Standard 803.3af PoE, and the two should not be intermixed. The CMMmicro can auto-negotiate speed to match inputs that are either 100Base-TX or 10Base-T, and either full duplex or half duplex, where the connected device is set to auto-negotiate. Alternatively, these parameters are settable.

A CMMmicro requires only one cable, terminating in an RJ-45 connector, for each connected module to distribute

- Ethernet signaling.
- power to as many as 8 co-located modules—APs, BHMs, or BHSs. Through a browser interface to the managed switch, ports can be powered or not.
- sync to APs and BHMs. The CMMmicro receives 1-pulse per second timing information from Global Positioning System (GPS) satellites through an antenna (included) and passes the timing pulse embedded in the 24-V power to the connected modules.

GPS status information is available at the CMMmicro, however

- CMMmicro provides time and date information to BHMs and APs if both the CMMmicro is operating on CMMmicro Release 2.1 or later and the AP/BHM is operating on System Release 4.2 or later. See Time Tab of the AP on Page 198.
- CMMmicro *does not* provide time and date information to BHMs and APs if either the CMMmicro is operating on a release earlier than CMMmicro Release 2.1 or the AP/BHM is operating on a release earlier than System Release 4.2.

A CMMmicro is pictured in Figure 11 and Figure 12.

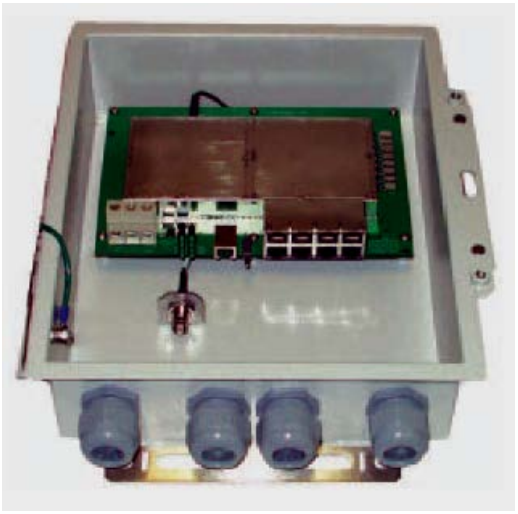


Figure 11: CMMmicro

Figure 12: Pole-mounted CMMmicro

This product is supported by its own dedicated user guide.

CMM4 (Part 1090CK, 1091AA)

The Cluster Management Module 4 (CMM4) provides power, GPS timing from an antenna that is included, and networking connections for an AP cluster, Backhauls, and Ethernet terrestrial feeds in a variety of configurations. The CMM4 provides reliable GPS network synchronization with an integrated solution that includes

- 9 access ports: eight 10/100Base-T ports and one copper 10/100/1000Base-T port
- a full featured Ethernet switch
- a Gigabit Ethernet port
- integrated lightning surge suppression on every data line, the GPS interface, the 29 V DC power inputs, and the coax line. These points include all RJ11 and RJ45 connectors.

The CMM4 has four major hardware components:

- the Cluster Controller. The controller injects power and synchronization on a per-port basis and is configured using a web or SNMP interface.
- a separate hardened Ethernet switch housed within the same weatherized enclosure. This switch integrates switching technology with its own separate web-based and SNMP management functions and provides a full array of networking features.
- the GPS system. This includes an integrated GPS board, an antenna, and brackets for pole mounting the antenna.
- the power supply unit. This is a 20-volt, 40-watt supply that outputs on two connectors.

The CMM4 supports:

- Power over Ethernet (PoE) using a proprietary 30- or 56-VDC scheme that *differs from* IEEE Standard 803.af.
- synchronization and date and time on each port (when connected radio devices are configured to receive synchronization via RJ11 sync port). When connected radio devices are receiving sync over the power port, only synchronization signaling is retrieved (date and time information may be synchronized by an NTP server in this configuration).
- Where the connected device is set to auto-negotiate, the CMM4 can auto-negotiate speed to match inputs that are either 100Base-TX or 10Base-T, and either full duplex or half duplex. Alternatively, these parameters are settable.
- management by a web browser, telnet, the console port, Prizm element management system, or a network manager that uses SNMP.
- dual power supply input redundancy. (Power supply is sold separately). The enclosure provides a 1-hole insert for a DC power cable gland.

This user guide introduces CMM4, but the dedicated *Cluster Management Module 4 (CMM4) User Guide* provides full documentation on this product, including installation instructions.

A CMM4 is pictured in Figure 13, and Figure 14..

Figure 13: CMM4 enclosure

Figure 14: CMM4

Optional Ethernet Switch in CMM4 - (Part 1090CK, 1091AA)

The Ethernet switch is a separate device enclosed within the CMM4 enclosure and connected to the CMM4 cluster controller via either the Gigabit port or one of the standard Ethernet ports. The switch may be accessed in any of three ways:

- through the administration console via RS-232 serial port. This access
  - requires either proximity to the switch or a dial-up connection.
  - is text-based, using Windows Hyperterminal.
  - does not require an IP address.
- through the web-based interface. This access requires that the IP address of the switch is accessible from the device on which the browser resides.
- through an external SNMP-based network management application. This access
  - communicates with switch functions at the MIB level.
  - requires SNMP element management software.

This is a hardened managed switch that provides

- 12 10/100Base-T ports, 8 of them powered
- 2 copper 10/100/1000Base-T (Gigabit) Ethernet port, copper connecting

The Ethernet Switch has many features not addressed in this document. For further information, either visit http://www.EtherWAN.com/manuals/es/EX96000_e1_Manual.pdf or see the EtherWAN switch manual provided with the CMM4.

Rackmount CMM4 (1092AA)

The Rackmount Cluster Management Module 4 (CMM4) provides power, GPS timing from an antenna that is included, and networking connections for an AP cluster, Backhauls, and Ethernet terrestrial feeds in a variety of configurations. The CMM4 provides reliable GPS network synchronization with an integrated solution that includes

- 9 access ports: eight 10/100Base-T ports and one copper 10/100/1000Base-T port
- a Gigabit Ethernet port
- integrated lightning surge suppression on every data line, the GPS interface, the 29 V DC power inputs, and the coax line. These points include all RJ11 and RJ45 connectors.

The CMM4 has four major hardware components:

- the Cluster Controller. The controller injects power and synchronization on a per-port basis and is configured using a web or SNMP interface.
- the GPS system. This includes an integrated GPS board, an antenna, and brackets for pole mounting the antenna.
- the power supply unit. This is a 20-volt, 40-watt supply that outputs on two connectors.

The CMM4 supports:

- Power over Ethernet (PoE) using a proprietary 30- or 56-VDC scheme that *differs from* IEEE Standard 803.af.
- synchronization and date and time on each port (when connected radio devices are configured to receive synchronization via RJ11 sync port). When connected radio devices are receiving sync over the power port, only synchronization signaling is retrieved (date and time information may be synchronized by an NTP server in this configuration).
- Where the connected device is set to auto-negotiate, the CMM4 can auto-negotiate speed to match inputs that are either 100Base-TX or 10Base-T, and either full duplex or half duplex. Alternatively, these parameters are settable.
- management by a web browser, telnet, the console port, an element management system, or a network manager that uses SNMP.
- dual power supply input redundancy. (Power supply is sold separately). The enclosure provides a 1-hole insert for a DC power cable gland.

The model 1092AA Rackmount CMM4 as shipped includes:

- Rackmounting accessories
- GPS Antenna and pole mount accessories

This user guide introduces CMM4, but the dedicated *Cluster Management Module 4 (CMM4) User Guide* provides full documentation on this product, including installation instructions.

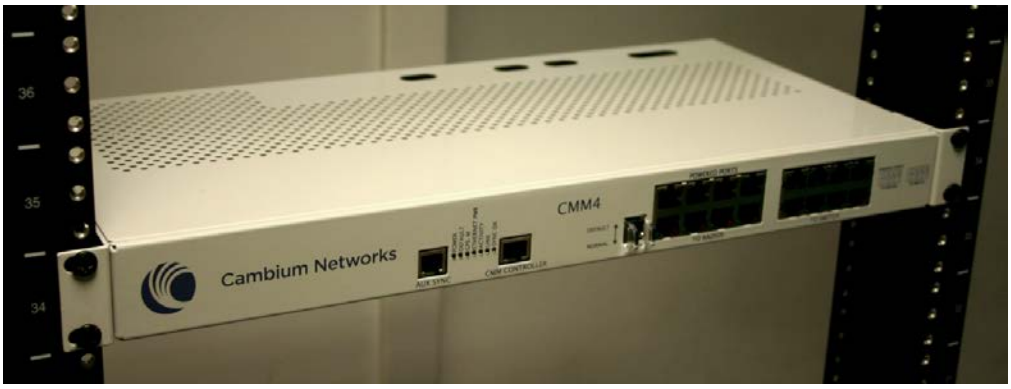


Figure 15: Rackmount CMM4

GPS Antenna (Part GPSANTPNM03D)

The Cambium GPS antenna provides either

- timing pulses to the CMMmicro or CMM4
- timing pulses and positioning information to the CMM2.

The GPS antenna is pictured in Figure 16.

Figure 16: Cambium GPS antenna

UNIVERSAL GPS (UGPS)

The UGPS provides network synchronization for smaller networks where a CMM may not be cost effective. The UGPS provides synchronization for one or two modules so that even remote areas at the edge of the network can operate with synchronization for improved performance. The UGPS works with all Cambium PMP radios. The UGPS has a small footprint and is easy to deploy.

Figure 17: Cambium UGPS antenna

The UGPS antenna is pictured in Figure 17**.**

Surge Suppressor (Part 600SS)

The 600SS Surge Suppressor provides a path to ground (Protective Earth ⏚) that reduces the risk to persons, buildings, and inside equipment from over-currents and over-voltages associated with lightning strikes. This accessory is RoHS compliant. A 600SS is pictured in Figure 18.

Figure 18: 600SS surge suppressor

Accessory Components

In addition to the above modules, the following accessories are available.

Power Supplies

The various power supplies are listed in Table 7.

Table 7: Power supply descriptions

To Power			For Use With	Part Number	VAC In	VDC Out	Line Cord Included
CMM	PMP FSK	PMP OFDM					
CMM4			PMP 49400 PMP 500	ACPS120W-02A	100 to 240	52.6	None.
CMM4 CMMmicro			PMP 100 PMP 54400	ACPS120WA	100 to 240	29	USA.
CMM4 CMMmicro			PMP 100 PMP 54400 and no power lead	ACPS120W-02A	100 to 240	29	None.
		49400 500	PoE and RJ-45 pass-through	SGPN4076	100 to 240	56	None.
	100	54400	network in USA or EU	ACPSSW-09B	90 to 240	29.5	USA, EU, UK.
	100	54400	network in Argentina	ACPSSW-10B	90 to 240	29.5	Argentina
	100	54400	network in Australia	ACPSSW-11B	90 to 240	29.5	Australia
	100	54400	network in China	ACPSSW-12C	90 to 240	29.5	China
	100		network in USA, Canada, or Mexico	ACPSSW-13A	90 to 240	24	USA, Canada, Mexico.

To Power			For Use With	Part Number	VAC In	VDC Out	Line Cord Included
CMM	PMP FSK	PMP OFDM					
		all	network in USA, Canada, or Mexico	ACPSSW-13B	90 to 240	29.5	USA, Canada, Mexico.

Region-compliant 56-V DC line cords for the power supplies are listed in Table 8.

Table 8: Line Cords for Power Supplies

Region	Part Number
Argentina	SGKN4419A
Australia	SGKN4425A
Canada	SGKN4427A
China-Mainland	SGKN4424A
Europe	SGKN4426A
India	SGKN4420A
Japan	SGKN4423A
Korea	SGKN4422A
Mexico	SGKN4427A
Pakistan	SGKN4420A
Singapore-United Kingdom	SGKN4421A
South Africa	SGKN4420A
USA	SGKN4427A

Passive Reflector Dish Assembly

A 27RD Passive Reflector Dish on both ends of a BH link extends the distance range of the link and provides a narrower beam width, which can reduce both received and transmitted interference. A 27RD on an SM extends the distance range in some bands (notably 5.7-GHz and 2.4-GHz) and can reduce both received and transmitted interference in all bands. The module support tube provides the proper offset focus angle. See Figure 19.

For 5.*x*-GHz radios, the reflector gain is 18dB and the 3 dB beam width is 6° in both azimuth and elevation. For 2.4-GHz radios, the reflector gain is 11dB and the 3 dB beam width is 17° in both azimuth and elevation.

Figure 19: 27RD with mounted module

LENS

The LENS product retrofits to a radio to

- improve range and resistance to interference, compared to those of the module with no reflector.
- provide less wind loading, easier mounting, and an appearance more consistent with the module form than has the reflector dish.

LENS focuses its beam in 60° azimuth and elevation and boosts signal gain by 9 to 10 dB. LENS is an option for 5.2-, 5.4-, and 5.7-GHz radios, but not an option for P7- through P9-series radios in the U.S.A. or Canada or for 2.4-GHz radios anywhere.

Viable use cases include all radio types (SM, BH, and AP), and installation in each case requires no tools. A dedicated user guide supports this product.

Currently, the radio types that support LEN retrofit are PTP 100, and PMP 100 and PMP 430 SM.

Figure 20: LENS mounted on a radio

Module Support Brackets

The SMMB1 support bracket facilitates mounting the SM to various surfaces of a structure and has slots through which chimney straps can be inserted. An SMMB1 is pictured in Figure 21. The SMMB1 is for use with an SM or an SM with a LENS. It is not for use with PMP 400 Series (OFDM) SMs or 900-MHz integrated or connectorized SMs, due to their greater weight and wind loading.

The SMMB2 is a heavy duty mounting bracket that comes with the 900-MHz integrated SM or AP, and with the 27D passive reflector. It is also available separately for use with 900-MHz connectorized SMs and APs, other connectorized modules, and 400 Series (OFDM) SMs.

The BH1209 is a pole-mount bracket kit for wireless Ethernet bridges.

Figure 21: SMMB1 SM support bracket

Cables

Modules that are currently or recently sold can auto-sense whether the Ethernet cable is wired as straight-through or crossover. Some modules that were sold earlier cannot. The MAC address, visible on the module, distinguishes whether the module can. All CMMmicros and CMM4s can auto-sense the cable scheme.

Where a non auto-sensing module is deployed

- a straight-through cable must be used for connection to a network interface card (NIC).
- a crossover cable must be used for connection to a hub, switch, or router.

Cambium-recommended Ethernet and sync cables can be ordered in lengths up to 328 ft (100 m) from Best-Tronics Manufacturing, Inc. at http://www.best-tronics.com/cambium.htm . These cables are listed in Table 9 and Table 10.

Table 9: Recommended outdoor UTP Category 5E cables

Best-Tronics Part #	Description
BT-0562	RJ-45 TO RJ-45; straight-through Ethernet cable
BT-0562S	RJ-45 TO RJ-45; shielded straight-through Ethernet cable
BT-0565	RJ-45 TO RJ-45; crossover Ethernet cable
BT-0565S	RJ-45 TO RJ-45; shielded crossover Ethernet cable
BT-0563	RJ-11 TO RJ-11; sync cable
BT-0563S	RJ-11 TO RJ-11; shielded sync cable
BT-0781S	RJ-45 to RJ-45; straight shielded Ethernet cable using outdoor STP Cat 5e cable, lower cost than plenum-rated, available only in black. Recommended for CMM4 to AP.

NOTE:
Shielded cable is strongly recommended for all AP cluster and BH installations.

Table 10: Recommended indoor UTP Category 5E cables

Best-Tronics Part #	Description
BT-0596	RJ-45 TO RJ-45; straight-through Ethernet cable
BT-0595	RJ-45 TO RJ-45; crossover Ethernet cable

Approved Ethernet cables can also be ordered as bulk cable:

- CA-0287
- CA-0287S (shielded)
- CA-0367 (lower cost, non-plenum-rated),
- CA-0367S (shielded, lower cost, non-plenum-rated)

Cambium-approved antenna cables can be ordered in lengths up to 100 ft (30.4 m), as listed in Table 11.

Table 11: Recommended antenna cables

Best-Tronics Part #	Description
BT-0564	N TO N GPS antenna cable for CMM2
BT-0716	BNC TO N GPS antenna cable for CMMmicro and CMM4

Category 5 Cable Tester

For purchase within the U.S.A., the CTCAT5-01 Cable Tester is available.

Override Plug

An override plug (sometimes called a default plug) is available to provide access to a module whose password and/or IP address have been forgotten. This plug allows the AP, SM, or BH to be accessed using IP address 169.254.1.1 and no password. During the override session, you can assign any new IP address and set either or both user passwords (display-only and/or full access) as well as make other parameter changes.

This plug is available from Best-Tronics Manufacturing, Inc. at http://www.best-tronics.com/cambium.htm as Part BT-0583 (RJ-11 Default Plug). Alternatively if you wish, you can fabricate an override plug. For instructions, see Procedure 34 on Page 433 and the pinout in

Figure 150 on Page 434.

Alignment Headset

The ACATHS-01 Alignment Headset facilitates the operation of precisely aiming an SM toward an AP (or a BHS toward a BHM). This device produces infinitely variable

- pitch, higher when the received signal is stronger.
- volume, louder when jitter is less.

An ACATHS-01 is pictured in Figure 22.

Pinouts for an alternative listening device are provided under Alignment Tone—Technical Details on Page 189.

Figure 22: ACATHS-01 alignment headset

Module Housing

The HSG-01 Plastic Housing is available for replacement of a damaged housing on a module that is otherwise functional. The HSG-01 is pictured in Figure 23.

The HSG-01 and all module housings of this design provide clearances for cable ties on the Ethernet and sync cables.

RECOMMENDATION:
Use 0.14" (40-lb tensile strength) cable ties to secure the Ethernet and sync cables to the cable guides on the module housing.

For the Ethernet cable tie, the Ethernet cable groove is molded lower at the top edge. For the sync cable tie, removal of a breakaway plug provides clearance for the sync cable, and removal of two breakaway side plates provides clearance for the sync cable tie.

Figure 23: HSG-01 Housing

NOTE:
No replacement housing is available for an OFDM radio.

Frequency Band Ranges

In the 2.4-, 5.2-, 5.4-, and 5.7-GHz frequency band ranges, APs, SMs, and wireless Ethernet bridges are available. APs and SMs are also available in the 900-MHz frequency band range. National restrictions may apply. See Regulatory and Legal Notices on Page 583.

To avoid self-interference, a network typically uses two or more of these ranges. For example, where properly arranged, all AP clusters and their respective SMs can use the 2.4-GHz range where the BH links use the 5.7-GHz range. In this scenario, subscriber links can span as far as 5 miles (8 km) with no reflector dishes, and the BH links can span as far as 35 miles (56 km) with reflector dishes on both ends or 16 miles (25 km) in 1X operation with LENS on both ends.

Within this example network, wherever the 2.4-GHz module is susceptible to interference from other sources, AP clusters and their linked SMs may use the 5.2-GHz range to span as far as 2 miles (3.2 km) with no reflector dishes. The network in this example takes advantage of frequency band range-specific characteristics of modules as follows:

- The 900-MHz modules cover a larger area, albeit with lower throughput, than modules of the other frequency bands. The 900-MHz modules can be used to
  - penetrate foliage
  - establish links that span greater distances
  - add subscribers
  - add overall throughput where modules of other frequency bands cannot be used (such as where interference would result or space on a tower is limited).
- The 2.4-GHz frequency band range supports AP/SM links of greater than 2-mile spans (with no reflectors).
- The 5.7-GHz frequency band range supports BH links that span as far as 35 miles.

Product Comparisons

Product Applications

The product applications per frequency band range are is summarized in Table 12.

Table 12: Product applications per frequency band range

Product	Frequency Band Range						
	900-MHz FSK	2.4-GHz FSK	4.9-GHz OFDM	5.2-GHz FSK	5.4-GHz FSK	5.4-GHz OFDM	5.7-GHz FSK
Access Point Module	•	•	•	•	•	•	•
Subscriber Module	•	•	•	•	•	•	•
Subscriber Module with Reflector[1]		•		•	•		•
Backhaul Module		•		•	•		•
Backhaul Module with Reflector[1]		•		•	•		•
CMMmicro	•	•	•	•	•	•	•
CMM2	•	•		•	•		•
CMM4	•	•	•	•	•	•	•

Product	Frequency Band Range						
	900-MHz FSK	2.4-GHz FSK	4.9-GHz OFDM	5.2-GHz FSK	5.4-GHz FSK	5.4-GHz OFDM	5.7-GHz FSK
Power supply	●	●	●	●	●	●	●
Surge suppressor	●	●	●	●	●	●	●

NOTES:

1. National or regional regulations may limit EIRP to the same as without a reflector, and therefore require Transmit Output Power to be reduced. In these cases
   - the reflector used with an SM reduces beamwidth to reduce interference, but *does not* increase the range of the link.
   - the reflector on both ends of a BH link reduces beamwidth to reduce interference and also increases the range of the link.

Link Performance and Encryption Comparisons

Encryption options are summarized in Table 13. Typical Line-of-Site (LOS) range and aggregate useful throughput for PMP links are summarized in Table 14. Typical Line-of-Site (LOS) range and aggregate useful throughput for PTP links are summarized in Table 15.

Table 13: Products with encryption options available per frequency band, PMP links

Frequency Band	Products available with the following encryption options	
	DES or none	AES or none
900 MHz	●	●
2.4 GHz @100 mW (ETSI)	●	●
2.4 GHz @ 1W	●	●
4.9 GHz OFDM	●	
5.2 GHz	●	●
5.4 GHz FSK	●	●
5.4 GHz OFDM	●	
5.7 GHz	●	●

Table 14: Typical range and throughput per frequency band, PMP links

Frequency Band		CAP 130				CAP 120, 49400, 54400			
		Range		Aggregate Throughput Mbps	Round-trip Latency msec	Range		Aggregate Throughput Mbps	Round-trip Latency msec
		no SM Reflector mi (km)	with SM Reflector mi (km)			no SM Reflector mi (km)	with SM Reflector mi (km)		
900 MHz[4]		40 (64)	na	4	15				
2.4 GHz ETSI		0.3 (0.5)	0.3 (0.5) [1]	14	6	0.6 (1)	0.6 (1) [1]	7	20
		0.6 (1)	0.6 (1) [1]	7	6				
2.4 GHz		2.5 (4)	7.5 (12)	14	6	5 (8)	15 (24)	7	20
		5 (8)	15 (24)	7	6				
4.9 GHz OFDM	1X					5 (8)		7	TBD
	2X					2.5 (4)		14	TBD
	3X					1.25 (2)		21	TBD
5.2 GHz		1 (1.6)	na[2]	14	6	2 (3.2)	na[2]	7	20
		2 (3.2)	na[2]	7	6				
5.4 GHz		1 (1.6)	1 (1.6) [3]	14	6	2 (3.2)	2 (3.2) [3]	7	20
		2 (3.2)	2 (3.2) [3]	7	6				
5.4 GHz OFDM	1X					5 (8)		7	TBD
	2X					2.5 (4)		14	TBD
	3X					1.25 (2)		21	TBD

Frequency Band	CAP 130				CAP 120, 49400, 54400			
	Range		Aggregate Throughput Mbps	Round-trip Latency msec	Range		Aggregate Throughput Mbps	Round-trip Latency msec
	no SM Reflector mi (km)	with SM Reflector mi (km)			no SM Reflector mi (km)	with SM Reflector mi (km)		
5.7 GHz	1 (1.6)	5 (8)	14	6	2 (3.2)	10 (16)	7	20
	2 (3.2)	10 (16)	7	6				

REFERENCED NOTES:

1. In Europe, 2.4-GHz ETSI and 5.4-GHz SMs can have a reflector added to focus the antenna pattern and reduce interference, but transmit output power must be reduced to maintain the same EIRP as without a reflector, so the throughput and range specs for PTMP links remain the same.
2. In the US and Canada, the use of a reflector with a full power radio in the 5.2-GHz frequency band is not allowed.
3. In US, Europe, and Australia, 5.4-GHz SMs can have a reflector added to focus the antenna pattern, reduce interference, and improve downlnk gain, but transmit output power must be reduced to maintain the same EIRP as without a reflector, so the throughput and range specs for PTMP links remain the same. Reflectors are not allowed on 5.4-GHz SMs in Canada at this time.
4. All 900-MHz APs are CAP 09130s.

GENERAL NOTES:

Range is affected by RF conditions, terrain, obstacles, buildings, and vegetation.

A CAP 130 has an aggregate (sum of uplink plus downlink) throughput or capacity of 14 Mbps, if RF conditions, range, and SM hardware version permit.

An CSM 130 has an aggregate sustained throughput of 14 Mbps if RF conditions and range permit.

A regular SM can burst to 14 Mbps if RF conditions and range permit, then run at 7 Mbps sustained throughput.

An OFDM SM has an aggregate throughput or capacity of 21 Mbps, if RF conditions and range permit.

Table 15: Typical range and throughput per frequency band, PTP links

Frequency Band		Modulation Rate (Mbps)	Throughput	
			No Reflectors	Both Reflectors
2.4 GHz @100 mW (ETSI)		10	7.5 Mbps to 2 km	7.5 Mbps to 16 km
		20	14 Mbps to 1 km	14 Mbps to 8 km
2.4 GHz @ 1W		10	7.5 Mbps to 5 mi (8 km)	7.5 Mbps to 35 mi (56 km)
		20	14 Mbps to 3 mi (5 km)	14 Mbps to 35 mi (56 km)
4.9 GHz OFDM	1X		7 Mbps to 5 mi (8 km)	
	2X		14 Mbps to 2.5 mi (4 km)	
	3X		21 Mbps to 1.25 mi (2 km)	
5.2 GHz		10	7.5 Mbps to 2 mi (3.2 km)	
		20		
5.2 GHz ER		10		7.5 Mbps to 10 mi (16 km)
		20		14 Mbps to 5 mi (8 km)
5.4 GHz		10	7.5 Mbps to 2 mi (3.2 km)	7.5 Mbps to 10 mi (16 km)[1]
		20	14 Mbps to 1 mi (1.6 km)	14 Mbps to 5 mi (8 km)[1]
5.4 GHz OFDM	1X		7 Mbps to 5 mi (8 km)	
	2X		14 Mbps to 2.5 mi (4 km)	
	3X		21 Mbps to 1.25 mi (2 km)	
5.7 GHz		10	7.5 Mbps to 2 mi (3.2 km)	7.5 Mbps to 35 mi (56 km)
		20	14 Mbps to 1 mi (1.6 km)	14 Mbps to 35 mi (56 km)

NOTES:

1. These ranges are with power reduced to within 1 W (30 dBm) EIRP.
2. Use the Link Estimator tool to estimate throughput for a given link.

Cluster Management Product Comparison

Cambium offers a choice among products for cluster management: CMM2, CMMmicro, CMM4, and CMM4 Rackmount. Your choice should be based on the installation environment and your requirements. The similarities and differences between these two products are summarized in Table 16.

Table 16: Cluster management product similarities and differences

Characteristic	CMM2	CMMmicro	CMM4	CMM4 Rackmount
Approximate size	17” H x 13” W x 6.5” D (43 cm H x 33 cm W x 7 cm D)	12” H x 10” W x 3” D (30 cm H x 25 cm W x 8 cm D)	20.75" H x "14.75" x W x "7.75" D (52.7 cm H x 37.5 cm W x 19.7 cm D)	19” x 9.5” x 1.75” or 1 Rack Space (48.25 cm x 24 cm x 4.5 cm
Approximate weight	25 lb (11.3 kg)	8 lb (3.5 kg)	14 lb (6.4 kg)	6.8 lbs. (3 kg)
Cabling	one Ethernet/power cable per radio. one sync cable per radio.	one Ethernet/power/sync cable per radio.	one Ethernet/power/sync cable per radio.	one Ethernet/power/sync cable per radio.
Network interconnection	8 Ethernet ports	8 Ethernet ports	8 Ethernet ports	8 Ethernet ports
Data throughput	auto-negotiates to full or half duplex	auto-negotiates to full or half duplex	auto-negotiates to full or half duplex	auto-negotiates to full or half duplex
Ethernet operating speed standard	auto-negotiates to 10Base-T or 100Base-TX	auto-negotiates to 10Base-T or 100Base-TX	auto-negotiates to 10Base-T or 100Base-TX	auto-negotiates to 10Base-T or 100Base-TX
Additional Ethernet ports	one for data feed one for local access (notebook computer)	none	one copper 10/100/1000Base-T	one copper 10/100/1000Base-T
Optional Ethernet switch	none	none	12 10/100Base-T ports 1 copper Gigabit port 1 fiber optic Gigabit port	12 10/100Base-T ports 1 copper Gigabit port 1 fiber optic Gigabit port
Power supply	integrated 24-V DC to power APs, BHs, and GPS receiver	external 24-V DC to power APs, BHs, and GPS receiver	20-v DC power output	20-v DC power output
SNMP management capability	none	provided	provided	provided

Characteristic	CMM2	CMMmicro	CMM4	CMM4 Rackmount
Sync (to prevent self-interference)	carried by the additional serial cable to each AP and BHM	embedded in power-over-Ethernet cable	embedded in power-over-Ethernet cable	embedded in power-over-Ethernet cable
Time & Date	carried by the additional serial cable to each AP and BHM	provided by NTP (Network Time Protocol). CMMmicro can be an NTP server.	provided by NTP (Network Time Protocol). CMM4 can be an NTP server.	provided by NTP (Network Time Protocol). CMM4 can be an NTP server.
Weatherized	enclosure and power supply	only the enclosure (not the power supply)	only the enclosure (not the power supply)	Indoor-use only
Web interface	none	web pages for status, configuration, GPS status, and other purposes	web pages for status, configuration, GPS status, and other purposes	web pages for status, configuration, GPS status, and other purposes
NOTE: Auto-negotiation of data throughput and Ethernet operating speed depend on the connected device being set to auto-negotiate as well.				

Each of these cluster management products is supported by its own dedicated user guide that which provides instructions for mounting and cabling the unit and verifying its connectivity to the network.

Antennas for 900-MHz Connectorized Modules

Like the 2.4-, 5.2-, 5.4-, and 5.7-GHz module, the 900-MHz connectorized module has

- the same housing.
- a covered Ethernet port.
- a utility port for an alignment headset, sync cable to CMM2, or override plug.

The 900-MHz AP or SM is available either

- as a connectorized unit with a 16-inch (approximately 40-cm) cable with a male N-type connector for connection to the antenna.
- with an integrated *horizontally*-polarized antenna in a different form factor.

Cambium has certified three connectorized flat panel antenna options. Cambium resells one of these. The three flat panel options are as follows:

- 10 dBi Maxrad Model # Z1681 (MP9027XFPT or Cambium AN900A), 26 dBm (390 mW). See http://www.maxrad.com/.

- 10 dBi Mars Model # MA-IS91-T2, 26 dBm (390 mW).
  See http://www.mars-antennas.com/.
- 10 dBi MTI Model # MT-2630003/N (MT-263003/N), 26 dBm (390 mW).
  See http://www.mtiwe.com/.

The attributes of each of these options are identical:

- gain—10 dBi
- polarization—vertical or horizontal
- cable—12-inch (30.5 cm)
- connector—female N-type
- beamwidth—approximately 60° vertical and 60° horizontal at 3 dBm

Cambium has certified other antennas, which are available through product resellers. The attributes of one of these other certified antennas include

- gain—10 dBi
- dimensions—12 x12 x 1 inches (30.5 x 30.5 x 2.5 cm)
- weight—3.3 lbs (1.5 kg)
- polarization—vertical or horizontal
- connector—female N-type
- beamwidth—approximately 60° vertical and 60° horizontal at 3 dBm

An additional certified antenna is as follows: 17 dBi Last Mile Gear Cyclone Model # 900-17H Yagi, 18 dBm (63 mW). See http://www.lastmilegear.com/.

Examples of these antennas are pictured in Figure 5 on Page 39.

See section Weatherproofing a 900 MHz Connectorized Antenna on page 394 for information on protecting the 900 MHz antenna from extreme weather conditiona.

Adjunctive Software Products

The capabilities of available applications and tools are summarized for comparison in Table 17. In this table, Prizm represents the element management system capabilities of Prizm, CNUT represents Canopy Network Updater Tool, WM represents Wireless Manager, and BAM represents the Bandwidth and Authentication Manager capabilities in Prizm.

Table 17: Applications and tools

Capability	Application or Tool			
	Prizm		CNUT	WM
	Prizm Server	BAM Server		
authenticates SMs	●	●		●
controls **authentication** in APs	●		●	●
manages **Committed Information Rate** (CIR)	●	●		●
has **dependency** on another application[3]			●	
automatically **discovers** elements	●		●	●
exports network information with hierarchy	●		●	●
supports user-defined **folder**-based operations	●		●	●
senses **FPGA version** on an element	●		●	●
upgrades **FPGA version** on an element			●	●
manages the **high-priority channel**	●	●		●
imports network information with hierarchy	●		●	●
interface to a higher-level network management system (NMS)	●			●
interface to an operations support system (OSS)	●			●
manages **Maximum Information Rate** (MIR)	●	●		●
automatically works from **root** (highest) level			●	
element **selection** can be individual or multiple	●	●	●	●
element **selection** can be criteria based	●			●
element **selection** can be user-defined branch	●		●	●
senses **software release** on an element	●		●	●
upgrades **software release** on an element			●	●

Capability	Application or Tool			
	Prizm		CNUT	WM
	Prizm Server	BAM Server		
manages **VLAN** parameters	•	•		•
provides access to element **web interface**	•			•

Wireless Manager (WM)

Cambium Networks Wireless Manager 4.0 is recommended for managing Cambium Point-to-Multipoint networks. You can achieve better uptime through better visibility of your network with the Cambium Wireless Manager. This network management software tool offers breakthrough map-based visualization capabilities using embedded Google maps, and combined with advanced configuration, provisioning, alerting and reporting features you can control your entire outdoor wireless network including Mesh Wide Area Network, and Point-to-Multipoint and Point-to-Point solutions as well as other SNMP enabled devices. With its powerful user interface you will not only be able to control your network's access, distribution and backhaul layers, but you will also have visibility to WLAN sites and be able to quickly launch indoor network management systems.

Some key features of Wireless Manager are:

- **Template-Based Configuration:** With Wireless Manager's user-defined templates you can accelerate the process for the configuration of the devices you add to your network resulting in quicker and easier deployments. The template-based functionality provides an automated way to configure large numbers of network devices with just a few mouse clicks, and can be scheduled to occur at any time via Wireless Manager's Task Scheduler.
- **Ultralight Thin Client:** With the growing mobile workforce it is important to have access to the status of your network at any time. With Wireless Manager you can view the status and performance of your entire wireless network via a compact web interface accessible by your smart phone.
- **Map-Based Visualization:** Wireless Manager overlays sophisticated real-time information about your network elements onto building layouts and dynamic Google maps. Visuals can be scaled to view an entire city or building or a specific area, floor or link.
- **High Availability Architecture Support:** Wireless Manager offers a high availability option, providing a highly reliable and redundant network management solution that ensures you always have management access to your network.
- **High Scalability:** The enhanced Wireless Manager offers you server scalability with support for up to 10,000 nodes as well as support for distributed server architecture.

Cambium's Wireless Manager is available for download at:
http://www.cambiumnetworks.com/support/planning/index.php?cat=1&type=0

Prizm

Network Definition and Element Discovery

Prizm allows the operator to partition the entire network into criteria-based subsets that can be independently managed. To assist in this task of defining networks, Prizm auto discovers network elements that are in

- user-defined IP address ranges
- SM-to-AP relationships with APs in the user-defined range
- BHS-to-BHM relationships with BHMs in the user-defined range.

For an AP, SM, wireless Ethernet bridge, CMMmicro, or CMM4, Prizm

- auto discovers the element to the extent possible.
- includes the element in the network tree.
- shows general information.
- shows software-driven information.
- supports software-specific operations.

For a generic element, Prizm

- auto discovers the element as only a generic network element.
- includes the element in the network tree.
- shows general information.
- shows events and alerts.
- charts port activity.

For passive elements (such as CMM2 or a non-manageable switch or hub), Prizm allows you to enter into the network tree a folder/group with name, asset/owner information, and descriptive information.

Monitoring and Fault Management

Prizm receives the traps that elements send and generates an alert for each of these. Prizm also allows the user to establish sets of criteria that would generate other alerts and trigger email notifications. Optionally, the user can specify a trap template. In this case, Prizm receives traps for generic elements in the network.

For any individual element that the user selects, Prizm offers text and graphed displays of element configuration parameters and performance statistics from an interval that the user specifies.

Element Management

Prizm allows the user to perform any of the following operations on any specified element or group of elements:

- Manage
  - large amounts of SNMP MIB data.
  - module passwords.
  - IP addresses.
  - other communications setup parameters.
  - site information: Site Name, Site Location, and Site Contact parameters.
- Reset the element.

BAM Subsystem in Prizm

Prizm integrates Bandwidth and Authentication Manager (BAM) functionality and supports the maintenance of authentication and bandwidth data on a RADIUS server.

Either of the following modes is available for the Prizm server, subject to licensing:

- BAM-only functionality, which manages only authentication, bandwidth service plans, and VLAN profiles of SMs.
- Full Prizm functionality, which manages attributes for all elements and authentication of SMs.

One difference between a service plan (or VLAN profile) and a configuration template that has the identical set of attributes is that the former is a long-term association whereas the latter is a one-time push to the element. When a service plan or VLAN profile is modified, the change is automatically applied to all elements that have the association. Another difference is that a configuration template cannot overwrite any values that a service plan or VLAN profile has set in an element.

Northbound Interface

Prizm provides three interfaces to higher-level systems:

- a Simple Network Management Protocol (SNMP) agent for integration with a network management system (NMS).
- a Simple Object Access Protocol (SOAP) XML-based application programming interface (API) for web services that supports integration with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system.
- console automation that allows such higher-level systems to launch and appropriately display the Prizm management console in GUI that is custom developed, using the *PrizmEMS™ Software Development Kit (SDK)*, which Cambium provides for this purpose.

Together these interfaces constitute the Northbound Interface feature. Prizm server administrator tasks and GUI developer information are provided in the *PrizmEMS™ Software Development Kit (SDK)*. This SDK also describes the how to define new element types and customize the Details views.

All other features of the Prizm product are supported by the dedicated document *Cambium Canopy Prizm User Guide* and associated release notes.

License Management

Under the original licensing regime, licenses were permanently tied to the Media Access Control (MAC) address of the equipment that was licensed or that used the licensed feature. Thus, they were not transferable. Under server-based license management, for some functionalities, Cambium offers licenses that

- float upon demand within the network.
- are tied to only the MAC address of the license management server for which they were ordered.

Server-based license management adds flexibility and makes available licenses that previously would have been held by de-commissioned equipment. License management technology from Macrovision, based on a FLEXnet™ Publisher license management model, provides the platform for server-based licensing. Capabilities that are authorized by licenses on this platform are *FLEXenabled* products. In this platform, the license management server checks and then either assigns or declines to assign a license in real time.

The total number of floating license keys that you need for any feature is the highest number that you will ever want to have simultaneously in use. The proper placement of these keys and the number and placement of fixed licenses are listed in Table 18.

Table 18: Correct placement of license keys

In This Release	License Key	Must Be in Directory	If This Platform	On This Server Device
Prizm for full mgmt	PrizmEMS Server, Element Pack BAM Server, AP Auth Server (APAS), Cap 2 Canopy Lite	C:\Canopy\Prizm\FLEXnet\license_files	Windows	LM server[1]
		/usr/local/Canopy/Prizm/FLEXnet/license_files	Enterprise Linux	
Prizm for BAM-only or redundant BAM	BAM Server, AP Auth Server (APAS), Cap 2 Canopy Lite	C:\Canopy\Prizm\FLEXnet\license_files	Windows	LM server[2]
		/usr/local/Canopy/Prizm/FLEXnet/license_files	Enterprise Linux	

NOTES:

1. One BAMServer key and one PrizmEMSServer key required per each full management Prizm server.
2. One key required per each deployed BAM server.

Specifications and Limitations

Radios

Radio specifications are provided at

- http://www.cambiumnetworks.com/products/index.php?id=ptp100 for PTP bridges.
- http://www.cambiumnetworks.com/products/index.php?id=pmp100 for PMP modules.

Cluster Management Products

CMM specifications are provided in the documents that support the various models of CMM.

600SS Surge Suppressor

600SS Surge Suppressor specifications are as follows:

Dimensions	H 5.2" x W 5.0" x D 1.7" (132 mm x 127 mm x 43.2 mm)
Space between mounting holes	4.24" (108 mm)
Size of Knockouts	0.75" (19 mm)
Weight	0.4 lbs
Operating Temperature	−40°C to +55°C (−40°F to 131°F)
Internal Connectors	RJ-45
Capacity	1500J peak energy dissipation with 10/10000 micro sec waveform
Digital Noise Isolation Option (to eliminate ground loops)	Yes

NOTE:
The 600SS surge surpressor is shipped in the “isolated” position (pin 4 isolated by 68V from protective earth). If packet error issues occur over the Ethernet link (verify by pinging the device through the 600SS), configure the 600SS to “grounded” position (by moving the 600SS switch from “isolated” to “ground”) to avoid ground loops that may be present in the system.

Chapter 6: Differentiating Among Components

Interpreting Model Number

The model number of a module typically represents

- the model number, which may indicate
  - radio frequency band range.
  - link distance range.
  - whether the module is a CAP/CSM 130 or not.
  - the factory-set encryption standard.
- the module type.
- whether the reflector dish is included.
- the antenna scheme of the module.
- whether adjustable power in the module is preset to low.
- the modulation capability.

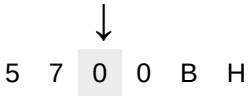
Radio Frequency Band Range

The leading two digits usually indicate the frequency band range in which the module can operate. For example, if the model number is 5700BH, then the frequency band range of the module is 5.7 GHz.

You cannot change the frequency band range of the module.

Link Distance Range or Series 130/09130

The third digit in the model number may indicate whether the module is an extended range, or a 130/09130 instead of a 120 in the PMP 100 Series. 1 indicates extended range, with power adjustable up to 23 dBm. 5 in the third position (5250AP, for example) indicates that the module is a CAP 130 or CSM 130. However, model numbering for 900-MHz APs and SMs differs from this general rule. All APs and SMs in this frequency band range are 09130, but none of their model numbers use 5 in the third position.

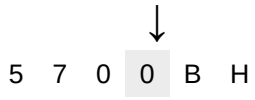


0 in the third position (5200AP, for example) indicates that the module is standard (not extended range, but rather capped to the maximum of 5 dBm, and not a CAP 130 or CSM 130).

You cannot change the link distance range of the module. However, you can license an SM to uncap its aggregate throughput (for capability of the CSM 130).

Encryption Standard or Frequency Band Range

The fourth digit in the model number usually indicates the encryption standard that was preset at the factory. 1 indicates the Advanced Encryption Standard (AES). 0 indicates the Data Encryption Standard (DES) standard. For example, if the model number is 5701BH, then transmissions from the module are encrypted according to AES. If the model number is 5700BH, then transmissions from the module are encrypted according to DES.



You cannot change the encryption basis (from DES to AES, for example), but you can enable or disable the encryption.

Module Type

The next two alpha characters indicate the module type. For example, CK indicates that the module is a Cluster Management Module.

The module type cannot be changed.

Reflector Added

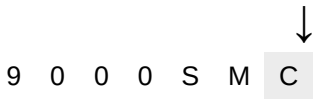
In specifications tables and price lists, the trailing characters RF or RF20 indicate that the associated information applies to the module being

- mounted to the 27RD Passive Reflector Dish, in the case of specifications.
- ordered with the 27RD Passive Reflector Dish, in the case of price lists.

However, this designation is not shown on either label of the module, and a module ordered with the dish can be deployed without the dish.

Antenna Scheme, Low Power Option, or Indoor Module

In specifications tables and price lists, the trailing character C indicates that the module is connectorized for an external antenna. CLP indicates that the module is low power and connectorized (for example, 2400SMCLP).



An F in this position indicates that the module has an integrated (internal) antenna with a band-pass, also known as interference migration, filter (for example, 9000APF). F2 in this position indicates that the module has a 2-channel band-pass filter (9000APF2). HZ indicates that the module has a horizontally polarized internal antenna (5200SMHZ).

A Q in this position indicates that the module has an integrated antenna and is designed for indoor deployment (for example, 9000SMQ).

You cannot transform a module from connectorized to internal antenna or from internal antenna to connectorized, but you may have flexibility in what external antenna you deploy with it.

Modulation Capability

A trailing 20 indicates that the module is capable of being set to either

- 20-Mbps modulation (aggregate throughput of 14 Mbps) for Full operation
- 10-Mbps modulation (aggregate throughput of 7 Mbps) for Lite operation.

The absence of a trailing 20 indicates that the module is capable of only 10-Mbps modulation (Lite).

Sorted Model Numbers

Model numbers of PMP 100, PMP 400, PTP 100, and PTP 200 series modules are listed in Table 19. Not all products are available in all regions or in all markets. Check with your distributor or reseller for availability.

Table 19: Model numbers

Range	Integrated Antenna				Connectorized for Antenna			
	Except 130 Series		130 PMP 100		Except 130 Series		130 PMP 100	
	DES	AES	DES	AES	DES	AES	DES	AES
900 MHz			9000AP 9000APF 9000APF2 9000SM 9000SMF 9000SMF2 9000SMQ	9001AP 9001APF 9001APF2 9001SM 9001SMF 9001SMF2			9000APC 9000SMC	9001APC 9001SMC
2.4 GHz	2400AP 2400SM 2400BH 2400BH20 2400BHRF 2400BHRF20	2401AP 2401SM 2401BH 2401BH20 2401BHRF 2401BHRF20	2450AP 2450SM	2451AP 2451SM	2400SMCLP	2401SMCLP		
4.9 GHz	4940AP 4940SM 4940BH	4941AP 4941SM 4941BH			4940APC 4940SMC 4940BHC	4941APC 4941SMC 4941BHC		
5.2 GHz	5200AP 5200APHZ 5200SM 5200SMHZ 5200BH 5210BHRF 5210BHRF20	5201AP 5201SM 5201BH 5211BH20 5211BHRF 5211BHRF20	5250AP 5250APHZ 5250SM 5250SMHZ	5251AP 5251SM				
5.4 GHz FSK	5400AP 5400APHZ 5400SM 5400SMHZ 5400BH 5400BH20 5400BHRF 5400BHRF20	5401AP 5401SM 5401BH 5401BH20 5401BHRF 5401BHRF20	5450AP 5450APHZ 5450SM 5450SMHZ	5451AP 5451SM				
5.4 GHz OFDM	5440AP 5440SM 5440BH	5441AP 5441SM 5441BH			5440APC 5440SMC 5440BHC	5441APC 5441SMC 5441BHC		
5.7 GHz	5700AP 5700APHZ 5700SM 5700SMHZ 5700BH 5700BH20 5700BHRF 5700BHRF20	5701AP 5701SM 5701BH 5701BH20 5701BHRF 5701BHRF20	5750AP 5750APHZ 5750SM 5750SMHZ	5751AP 5751SM	5700APC 5700BHC 5700BHC20	5701APC 5701BHC	5750APC	5751APC

Interpreting Electronic Serial Number (ESN)

Module labels contain a product serial number that could be significant in your dealings with Cambium or your supply chain. This is the electronic serial number (ESN), also known as the Media Access Control (MAC) address, of the module. This hexadecimal number identifies the module in

- communications between modules.
- the data that modules store about each other (for example, in the **Registered To** field).
- the data that the BAM software applies to manage authentication and bandwidth.
- Prizm auto discovery of SMs through the AP (or BHS through the BHM).
- software upgrades performed by CNUT.
- information that CNUT passes to external tools.

Finding the Model (Part) Number and ESN

The labels and locations of module model (part) numbers and ESNs are shown in Table 20.

Table 20: Labels and locations of model (part) numbers and ESNs

Numeric String	Label and Location	
	Older Modules	Newer Modules
Model number	**PN** outside	**Model #** outside
ESN/MAC address	**S/N** inside	**ESN** outside

Chapter 7: Link Characteristics

Understanding Bandwidth Management

Downlink Frame

A full frame consists of a downlink frame and an uplink frame. The downlink frame transmitted from the AP consists of

- a beacon
- an uplink map that tells each SM which slots it can use in the next uplink frame
- broadcast and per-SM data.

Each SM retrieves broadcast data and data addressed to that SM and passes that data through its Ethernet port to connected devices.

The beacon communicates

- timing
- ratio of uplink to downlink allocation
- ESN of the AP
- color code
- protocol (point-to-point or point-to-multipoint)
- number of registered SMs
- frame number
- number of reserved control slots
- air delay, subject to the value of the Max Range parameter in the AP.

Uplink Frame

The uplink frame transmitted from the SMs consists of

- per-SM data in slots assigned by the uplink map in the previous downlink frame
- bandwidth requests for data slots in future uplink frames.

Bandwidth requests are sent as control slots, which are half the size of a data slot. The operator configures a number of reserved control slots. In addition to the reserved control slots, space in any data slots in a given uplink frame not assigned by the uplink map is also available for bandwidth requests.

An SM makes a bandwidth request when it has data to transmit. Bandwidth requests are contention requests and are the only part of the Media Access Layer that uses contention. If two or more SMs make bandwidth requests using the same control slot (or half-unused-data slot), it is likely the AP will not be able to understand the requests. The SMs retransmit any bandwidth requests that do not result in assignments in the uplink map.

Slot Calculation

The frame consists of slots which hold 64-byte fragments of packet data. The number of uplink and downlink data slots is determined by

- the **Downlink Data** % configured by the operator, which determines the ratio of downlink to uplink data slots.
- the **Max Range** setting configured by the operator, which determines how much time in the frame must be reserved for air delay and not used for data.
- the number of reserved **Control Slots** configured by the operator. Control slots are half the size of data slots and every other reserved control slot (starting with either the first or second, depending on how the **Max Range** setting has influenced frame structure) reduces the number of data slots by one.

Startup Sequence

When an SM boots, the following sequence occurs:

1. The SM detects the beacon slot from an AP.
2. The SM synchronizes with the AP.
3. If an authentication server is configured on the AP, and the AP is licensed for authentication, then
   a) the AP sends a Registration Request message to the authentication server for authentication.
   b) following a successful challenge, the authentication server returns an Authentication Grant message to the AP.
   c) the AP sends a Registration Grant to the SM.

If an authentication server is not configured on the AP, or if the AP is not licensed for authentication, then the AP simply returns the Registration Grant to the SM.

This Registration Grant includes the air delay (distance) between the AP and SM. The SMs are at various distances from the AP, and each of them uses its air delay value to determine when to begin its uplink transmission. This results in uplink transmissions from multiple SMs at various distances all being in sync when the AP receives them.

Data Transfer Capacity

Modules use Time Division Duplex (TDD) on a common frequency to divide frames for uplink (orange) and downlink (green) usage, as shown in Figure 24.

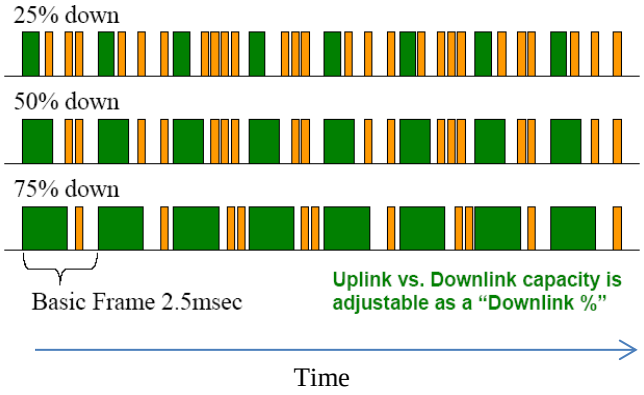


Figure 24: TDD dividing frames

Maximum Information Rate (MIR) Parameters

Point-to-multipoint links use the following four MIR parameters for bandwidth management:

- Sustained Uplink Data Rate (kbps)
- Uplink Burst Allocation (kb)
- Sustained Downlink Data Rate (kbps)
- Downlink Burst Allocation (kb)

You can independently set each of these parameters per AP or per SM.

Token Bucket Algorithm

The software uses a *token bucket* algorithm that

- stores credits (tokens) for the SM to spend on bandwidth for reception or transmission.
- drains tokens during reception or transmission.
- refills with tokens at the sustained rate set by the network operator.

For each token, the SM can send toward the network in the uplink (or the AP can send toward the SM in the downlink) an equivalent number of kilobits. Two buckets determine the permitted throughput: one in the SM for uplink and one in the AP for downlink.

The applicable set of **Uplink Burst Allocation** and **Downlink Burst Allocation** parameters determine the *number* of tokens that can fill each bucket. When the SM transmits (or the AP transmits) a packet, the equivalent number of tokens is removed from the uplink (or downlink) bucket.

Except when full, the bucket is continuously being refilled with tokens at *rates* that the applicable set of **Sustained Uplink Data Rate** and **Sustained Downlink Data Rate** parameters specify. The bucket often drains at a rate that is much faster than the sustained data rate but can refill at only the sustained data rate. Thus, the effects of the allocation and rate parameters on packet delay are as follows:

- the burst allocation affects how many kilobits are processed before packet delay is imposed.
- the sustained data rate affects the packet delay that is imposed.

Which set of these MIR parameters are applicable depends on the interactions of other parameter values. These interactions are described under Setting the Configuration Source on Page 324. Also, where the **Configuration Source** parameter setting in the AP specifies that BAM values should be used, they are used only if Prizm is configured to send the values that it stores for the MIR parameters.

MIR Data Entry Checking

Uplink and downlink MIR is enforced as shown in Figure 25.

NOTE:
In these figures, *entry* refers to the setting in the data rate parameter, not the burst allocation parameter.

$$\text{uplink cap enforced} = \frac{\text{uplink entry} \times \text{aggregate cap for the SM}}{\text{uplink entry} + \text{downlink entry}}$$

$$\text{downlink cap enforced} = \frac{\text{downlink entry} \times \text{aggregate cap for the SM}}{\text{uplink entry} + \text{downlink entry}}$$

Figure 25: Uplink and downlink rate caps adjusted to apply aggregate cap

For example, in the SM, if you set the **Sustained Uplink Data Rate** parameter to 2,000 kbps and the **Sustained Downlink Data Rate** parameter to 10,000 kbps, then the uplink and downlink MIR that will be enforced for the SM can be calculated as shown in Figure 26.

$$\text{uplink cap enforced} = \frac{2{,}000 \text{ kbps} \times 7{,}000 \text{ kbps}}{2{,}000 \text{ kbps} + 10{,}000 \text{ kbps}} = 1{,}167 \text{ kbps}$$

$$\text{downlink cap enforced} = \frac{10{,}000 \text{ kbps} \times 7{,}000 \text{ kbps}}{2{,}000 \text{ kbps} + 10{,}000 \text{ kbps}} = 5{,}833 \text{ kbps}$$

Figure 26: Uplink and downlink rate cap adjustment example

In this example case, the derived 1,167-kbps uplink and 5,833-kbps downlink MIR sum to the fixed 7,000-kbps aggregate cap of the SM.

Committed Information Rate

The Committed Information Rate (CIR) capability feature enables the service provider to guarantee to any subscriber that bandwidth will never decrease to below a specified minimum, unless CIR is oversubscribed. Bandwidth can be, and typically will be, higher than the minimum, but this guarantee helps the WISP to attract and retain subscribers.

CIR configuration is supported as follows:

- The GUI allows you to view and change CIR configuration parameters per SM.
- When an SM successfully registers and authenticates, if the authentication server has CIR configuration data for the SM, then messages make the CIR configuration available to the SM, depending on the Configuration Source setting. (See Setting the Configuration Source on Page 324.)
- The operator can disable the CIR feature in the SM without deleting the CIR configuration data.

Bandwidth from the SM Perspective

In the SM, normal web browsing, e-mail, small file transfers, and short streaming video are rarely rate limited with practical bandwidth management (QoS) settings. When the SM processes large downloads such as software upgrades and long streaming video or a series of medium-size downloads, the bucket rapidly drains, the burst limit is reached, and some packets are delayed. The subscriber experience is more affected in cases where the traffic is more latency sensitive.

Example download times for various arbitrary tiers of service are shown in Table 64 on Page 441 and Table 65 on Page 442.

Interaction of Burst Allocation and Sustained Data Rate Settings

If the Burst Allocation is set to 1200 kb and the Sustained Data Rate is set to 128 kbps, a data burst of 1000 kb is transmitted at full speed because the Burst Allocation is set high enough. After the burst, the bucket experiences a significant refill at the Sustained Data Rate. This configuration uses the advantage of the settable Burst Allocation.

If both the Burst Allocation and the Sustained Data Rate are set to 128 kb, a burst is limited to the Burst Allocation value. This configuration does not take advantage of the settable Burst Allocation.

If the Burst Allocation is set to 128 kb and the Sustained Data Rate is set to 256 kbps, the actual rate will be the burst allocation (but in kbps). As above, this configuration does not take advantage of the settable Burst Allocation.

High-priority Bandwidth

To support low-latency traffic such as VoIP (Voice over IP) or video, the system implements a high-priority channel. This channel does not affect the inherent latencies in the system but allows high-priority traffic to be immediately served. The high-priority pipe separates low-latency traffic from traffic that is latency tolerant, such as standard web traffic and file downloads.

IMPORTANT!

The number of channels available to the AP is reduced by the number of SMs configured for the high-priority channel. With this feature enabled on all SMs, an AP can support 100 SMs (instead of 200).

A module prioritizes traffic by

- reading the Low Latency bit (Bit 3) in the IPv4 Type of Service (ToS) byte in a received packet.
- reading the 802.1p field of the 802.1Q header in a received packet, where VLAN is enabled on the module.
- comparing the 6-bit Differentiated Services Code Point (DSCP) field in the ToS byte of a received packet to a corresponding value in the Diffserv tab of the Configuration page of the module.

Low Latency Bit

Bit 3 is set by a device outside the system. In the uplink frame, the SM monitors Bit 3. If this bit is set, then

- the SM prioritizes this traffic in its high-priority queue according to AP configuration settings for the high-priority channel.
- the system sends the packet on the high-priority channel and services this channel before any normal traffic.

802.1P Field

See Priority on VLANs (802.1p) on Page 169.

DSCP Field

Like Bit 3 of the original IPv4 ToS byte, the DSCP field (Bits 0 through 5) in the redefined ToS byte is set by a device outside the system. A packets contains no flag that indicates whether the encoding is for the Low Latency bit or the DSCP field. For this reason, you must ensure that all elements in your trusted domain, including routers and endpoints, set and read the ToS byte with the same scheme.

Modules monitor ToS bytes with DSCP fields, but with the following differences:

- The 6-bit length of the field allows it to specify one of 64 service differentiations.
- These correlate to 64 individual (**CodePoint**) parameters in the Diffserv tab of the Configuration page.
- Per RFC 2474, 3 of these 64 are preset and cannot be changed. (See http://www.faqs.org/rfcs/rfc1902.html.)
- For any or all of the remaining 61 CodePoint parameters, you can specify a value of
  - 0 through 3 for low-priority handling.
  - 4 through 7 for high-priority handling.

RECOMMENDATION:
Ensure that your Differentiated Services domain boundary nodes mark any entering packet, as needed, so that it specifies the appropriate Code Point for that traffic and domain. This prevents theft of service level.

An example of the Diffserv tab in the Configuration page and parameter descriptions are provided under Diffserv Tab of the AP on Page 270. This tab and its rules are identical from module type to module type. However, any of the 61 configurable Code Points can be set to a different value from module to module, thus defining unique per-hop behavior for some traffic.

This tab in the AP and BHM sets the priorities for the various packets in the downstream (sent from the public network). This tab in the SM and BHS sets the priorities for the various packets in the upstream (sent to the public network).

Typically, some SMs attach to older devices that use the ToS byte as originally formatted, and others to newer devices that use the DSCP field. The *default* values in the Diffserv tab allow your modules to prioritize traffic from the older devices roughly the same as they traditionally have. However, these default values may result in more high-priority traffic as DSCP fields from the newer devices are read and handled. So, after making any changes in the Diffserv tab, carefully monitor the high-priority channel for high packet rates

- in SMs that you have identified as those to initially set and watch.
- across your network when you have broadly implemented Code Point values, such as via SNMP.

Traffic Scheduling

This release requires APs, BHs, and AES SMs to be Series P9 or later hardware.[2] The characteristics of traffic scheduling in a sector are summarized in Table 21.

Table 21: Characteristics of traffic scheduling

Category	Factor	Treatment
Throughput	Aggregate throughput, less additional overhead	14 Mbps
Latency	Number of frames required for the scheduling process	1
	Round-trip latency[1]	≈ 6 ms
	AP broadcast the download schedule	No

[2] See Designations for Hardware in Radios on Page 381.

Category	Factor	Treatment
High-priority Channel	Allocation for *uplink* high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Allocation for *downlink* high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Order of transmission	1. CIR high-priority 2. CIR low-priority 3. Other high-priority 4. Other low-priority
Transmit Frame Spreading	Support for Transmit Frame Spreading feature	In Release 7.0 and later
CIR	Capability	In all releases
NOTES: 1. For 2.4- and 5.*n*-GHz modules.		

CAUTION!
Power requirements affect the recommended maximums for power cord length feeding the CMMmicro or CMM4. See the dedicated user guide that supports the CMM that you are deploying. However, the requirements *do not* affect the maximums for the CMM2.

Packets that have a priority of 4 to 7 in either the DSCP or a VLAN 802.1p tag are automatically sent on the high-priority channel, but only where the high-priority channel is enabled.

2X Operation

A General tab option in both CSM 130s and hardware series P9 and greater CSM 120s provides double the aggregate throughput for SMs that are nearer than half of the maximum typical range from the AP. The requirements of this feature are as follows:

- The AP must be a CAP 130 (Advantage AP).
- The SM must be near the AP, roughly half the range of 1X.
- The SM must be of the P9 hardware series or later and enabled for hardware scheduling. See Designations for Hardware on Page 425.
- The **2X Rate** parameter in the SM must be set to enabled. This is the default setting.

- The amount of noise and multipath must be low enough to allow the receiver in the 6 dB less sensitive (2X) state to maintain a high carrier-to-interference (C/I) ratio.

The flexibility of this feature is as follows:

- At the time of registration, signaling is at the 1X rate. However, if the above requirements are all met, then the SM switches to 2X.
- Thereafter, whenever RF conditions are unfavorable for 2X operation, the SM switches to 1X. When favorable RF conditions allow, the SM switches back to 2X, if user data is present at that time.
- Similarly, whenever no user data is present, the SM switches to 1X. When user data flow resumes, the SM switches back to 2X, if RF conditions allow.
- Both links for the SM (uplink and downlink) are independent for this feature. (One can be operating at 2X operation while the other is operating at 1X.)
- Other SMs in the sector can be communicating with the AP at the other modulation rate.
- Although subscribers with CSM 120s realize higher bursts, and subscribers with CSM 130s and CSM 09130s realize both higher burst and higher sustained throughput, the network operator realizes higher sector throughput capacity in the AP.

The effect of 2X operation on aggregate throughput for the SM is indicated in Table 22.

Table 22: Effect of 2X operation on throughput for the SM

Type of SM	Typical Aggregate Rates[1]	
	Sustained[2]	Burst[2]
CSM 09130	4 Mbps	4 Mbps
CSM 120 with at least P9 Hardware Series	7 Mbps	14 Mbps
CSM 54400	14 Mbps	14 Mbps

NOTES:

1. Subject to competition among all SMs in the sector.
2. Can be less if limited by the value of **Downlink Data** set in the Radio tab of the Configuration page in the AP.

Competition for Bandwidth

When multiple SMs vie for bandwidth, the AP divides its bandwidth among them, considering their effective CIR and MIR values. However, 2X operation uses bandwidth twice as efficiently as 1X, even where MIR values apply. This is because, in 2X operation, the modules transmit their data in 4-level frequency shift keying (FSK), not
2-level as they would in 1X operation. This moves twice the data per slot. Thus, for the sum of all bandwidth that 2X-eligible customers use, the bandwidth available to the remaining customers increases by half of that sum when these eligible customers are transmitting and receiving in 2X operation.

Checking Link Efficiencies in 2X Operation

Unlike in 1X operation, efficiencies below 90% on the Link Capacity Test tab in the Tools web page of the SM may be acceptable for stable operation. An efficiency of 60% in 2X operation is equivalent to an efficiency of 120% in 1X. If you read efficiency between 60% and 90%, check the status of 2X operation (as described below) to confirm that the link is operating at 2X.

Since received signal strength typically varies over time, you should perform link tests at various times of day and on various days of the week. Efficiencies should consistently be 60% or greater for 2X operation. You may be able to achieve better efficiencies by re-aiming the SM, mounting it elsewhere, or adding a reflector dish.

Checking the Status of 2X Operation

The Session Status tab in the Home page of the AP provides operation status information about each *SM-to-AP* link. Under the MAC address of each SM, the data in this tab includes a line such as the following:

RATE : VC 19 Rate 2X/2X VC 255 Rate 2X/1X

Interpret this information is as follows:

- VC means virtual channel. If one VC is displayed, the high-priority channel is disabled. If two are displayed, the high-priority channel is enabled and is using the higher number VC (255 in the above example).
- 2X/2X indicates that the SM-to-AP link is in 2X operation.
- 2X/1X indicates that the SM is capable of 2X operation but the SM-to-AP link is in 1X operation. This can be for either of the following reasons:
  - The SM has not sent data on the channel yet.
  - The received signal does not support 2X operation.
- 1X/1X indicates that the SM is capable of only 1X operation. This can be for either of the following reasons:
  - The SM does not support 2X operation (SM is of the hardware series P7 or P8).
  - The **2X Rate** parameter is disabled in the General tab of the Configuration page in the SM or the AP.

CAUTION!

2X operation requires approximately 3 to 5% more power than 1X operation. This additional power affects the recommended maximum for power cord length feeding the CMMmicro or CMM4. See the dedicated user guide that supports the CMM model that you are deploying. However, 2X operation *does not* affect the maximums for the CMM2.

Disabling 2X Operation

Disabling 2X operation for an SM can be helpful for alignment, troubleshooting, or preventing frequent automatic switches between 2X and 1X, where RF conditions are only marginally favorable to 2X. The ability to disable 2X for an SM is inherent since the 2X Operation feature was introduced.

Disabling 2X operation for a sector can be helpful for identifying a baseline for 1X-to-2X comparison, broader troubleshooting activities, or forcing all SMs to 1X rather than disabling 2X in each SM. The General tab of the Configuration page in the AP provides a **2X Rate** parameter:

- If you click **Disable**, then **Save Changes** and **Reboot**, 2X operation is disabled for the sector, regardless of the 2X Rate setting in each SM.
- If you later click **Enable**, then **Save Changes** and **Reboot**, 2X operation is enabled in the sector for SMs with 2X Rate enabled on their Configuration>General page. SMs with 2X Rate disabled on their Configuration>General page (or P7 or P8 SMs that don't support 2X Rate) will only operate at 1X.

If you want to cap the bandwidth usage of certain SMs, it is generally wiser to use the Maximum Information Rate (MIR) parameters of those SMs to do so, instead of locking down the operation rate for the entire sector. See Maximum Information Rate (MIR) Parameters on Page 83.

3X Operation

OFDM modules offer an additional modulation scheme that provides 3X operation as an alternative to 1X or 2X operation. In clear space, 3X operation is possible over half the range of 2X (which means it is possible over one-fourth the range of 1X). However, in NLOS installations, multipathing may be the predominant RF issue, not free-space attenuation, so the relationship between 1X, 2X, and 3X range may differ from clear space situations.

The effect of operation rate on the performance of OFDM modules in 10-MHz channel width deployment is generalized in Table 23. Aggregate throughput refers to the sum of the uplink throughput plus the downlink throughput.

Table 23: OFDM module performance at 1X, 2X, and 3X operation

Product	Performance Specification	Performance Details		
		1X	2X	3X
PMP 49400 PTP 49200	Modulation	QPSK	16 QAM	64 QAM
	Typical Maximum Range	15 mi (24 km)	4 mi (6.5 km)	2 mi (3.2 km)
	Typical Maximum Aggregate Throughput	7 Mbps	14 Mbps	20 Mbps
	Nominal Receive Sensitivity including FEC	−89 dBm	−80 dBm	−71 dBm
	Latency	5−7 ms	5−7 ms	5−7 ms
PMP 54400 PTP 54200	Modulation	QPSK	16 QAM	64 QAM
	Typical Maximum Range	5 mi (8 km)	2.5 mi (4 km)	1.25 mi (2 km)
	Typical Maximum Aggregate Throughput	7 Mbps	14 Mbps	20 Mbps PMP 21 Mbps PTP
	Nominal Receive Sensitivity including FEC	−89 dBm	−78 dBm	−70 dBm
	Latency	5−7 ms	5−7 ms	5−7 ms
PMP 58430	Modulation	QPSK	16 QAM	64 QAM
	Typical Maximum Range	7 mi (11.2 km)	3 mi (4.8 km)	2 mi (3.2 km)
	Typical Maximum Aggregate Throughput	7.5 Mbps	15 Mbps	22.5 Mbps
	Nominal Receive Sensitivity including FEC	−89 dBm	−78 dBm	−70 dBm
	Latency	5−7 ms	5−7 ms	5−7 ms

3X operation is configured on an OFDM module's Configuration => General page using the **Dynamic Rate Adapt** drop-down list under MAC Control Parameters.

For information such as how to check link efficiencies or the status of 3X operation or how to disable 3X operation, see the PMP 400-430 and PTP 200-230 User Guide.

Engineering for 2X and 3X Operation

The following priorities should guide your implementation of 2X and 3X operation:

- In the near quarter of the distance range of the AP
  - identify the customers who use the most bandwidth on OFDM SMs.
  - enable their SMs first for 3X operation.
- In the near half of the distance range of the AP
  - identify the customers who use the most bandwidth.

  - enable their SMs first for 2X operation.
- When you have deployable P7 and P8 SMs, *do not* deploy CSM 130s, CSM 09130s, or CSM 120 P9s beyond half the distance range of the AP. At this distance, steady and reliable 2X operation typically is not achievable. Deploy the P7 and P8 SMs here.
- Wherever practical, implement
  - 10 MHz of channel separation for 3X operation.
  - 25 MHz of channel separation for 2X operation.

Understanding Synchronization

The system uses Time Division Duplexing (TDD) - one channel alternately transmits and receives - rather than using one channel for transmitting and a second channel for receiving. To accomplish TDD, the AP must provide sync to its SMs – it must keep them in sync. Furthermore, co-located APs must be synced together - an unsynchronized AP that transmits during the receive cycle of a co-located AP can prevent that second AP from being able to decode the signals from its SMs. In addition, across a geographical area, APs that can “hear” each other benefit from using a common sync to further reduce self-interference within the network.

GPS Synchronization

The Navigation Satellite Timing and Ranging (NAVSTAR) Global Positioning System (GPS) uses 24 satellites to relay information for precise derivation of position and time.

The cluster management module (CMM) contains a Cambium Oncore GPS Receiver. The CMM is a critical element in the operation of the system. At one AP cluster site or throughout an entire wireless system, the CMM provides a GPS timing pulse to each module, synchronizing the network transmission cycles.

The Oncore GPS Receiver tracks eight or more satellites. The CMM uses the signal from at least four of these satellites to generate a one-second interval clock that has a rise time of 100 nsec. This clock directly synchronizes APs and BHMs which, in turn, synchronize the SMs and BHSs in the network.

The Oncore GPS Receiver also provides

- the latitude and longitude of the GPS antenna (co-located with the CMM)
- the number of satellites that are being tracked
- the number of satellites that are available
- the date
- the time in Universal Coordinated Time (UCT)
- the altitude of the GPS antenna
- other information that can be used to diagnose network problems.

Alternative to GPS Sync

A link can operate without *GPS* sync, but cannot operate without sync. The alternative to GPS sync is to configure the AP or BHM in the link to generate a sync pulse to pass to the SM or BHS, respectively. Depending on the RF environment in which the link operates, this latter alternative may or may not be plausible.

For example, in Figure 27, AP4

- is not synchronized with any of the other APs.
- is transmitting nearby the other APs while they are expecting to receive SM transmissions from a maximum distance.

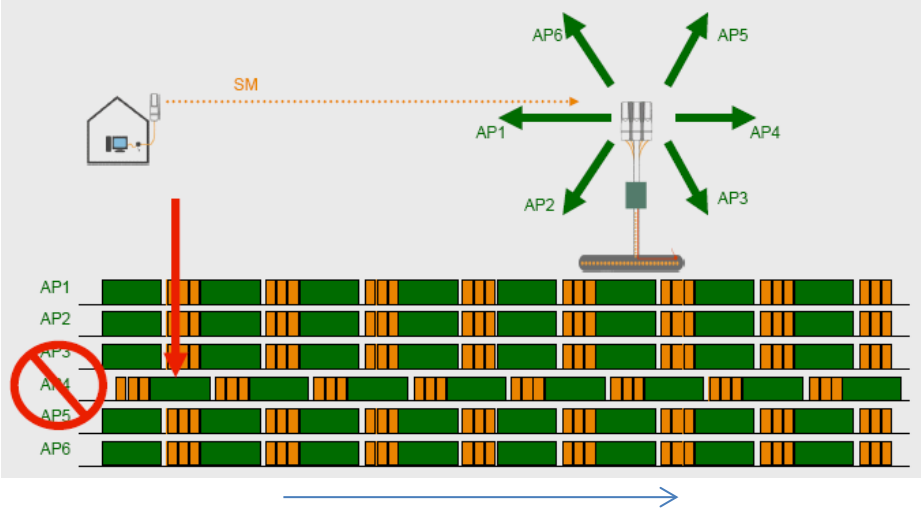


Figure 27: One unsynchronized AP in cluster

The result is self-interference. In this scenario, the self-interference can be avoided only by synchronizing the TDD transmit cycles of all APs that operate in the same frequency band.

An AP that is isolated by at least 5 miles (8 km) from any other equipment, or a BHM in an isolated standalone BH link can generate and pass sync pulse without GPS timing and not risk that interference will result from the generated sync. In any other type of link, sync should be derived from GPS timing.

NOTE:
The OFDM Series BHMs generate their own sync. For more information about these modules, see the user guides that support them. Titles are listed under Products Not Covered by This User Guide on Page 24.

Advantage of GPS Sync

Although the embedded timing generation capability of the AP and BHM keeps a precise clock, no trigger exists to start the clock at the same moment in each AP of a cluster. So, the individual AP can synchronize communications between itself and registered SMs, but cannot synchronize itself with other modules, except by GPS timing (shown in Figure 28).

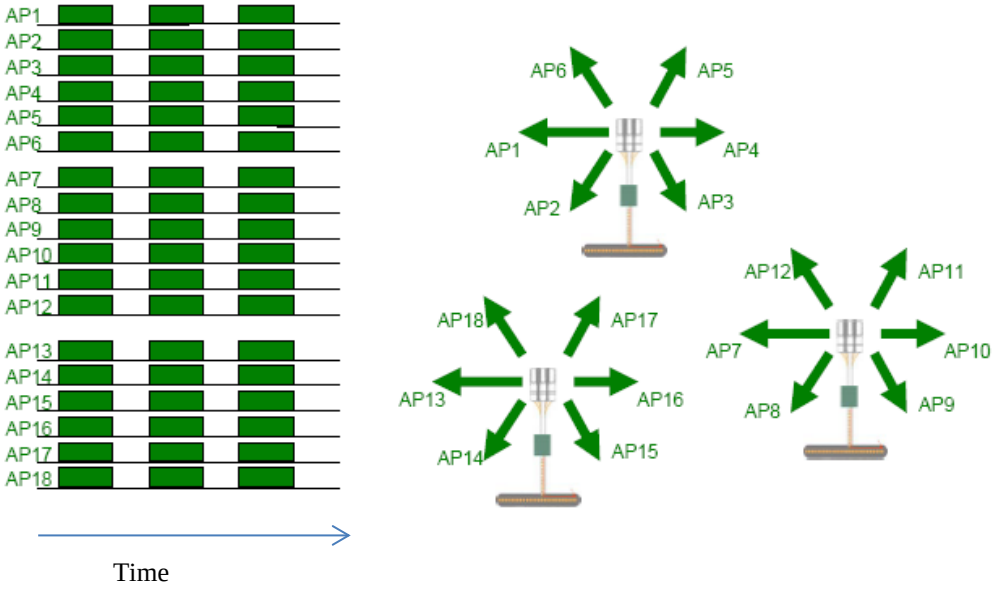


Figure 28: GPS timing throughout the network (FSK shown)

Passing Sync in a Single Hop

Network sync can be passed in a single hop in the following network designs:

- Design 1
  - A CMM provides sync to a co-located AP.
  - This AP sends the sync over the air to SMs.
- Design 2
  - A CMM provides sync to a co-located BH timing master.
  - This BH timing master sends the sync over the air to a BH timing slave.

Passing Sync in an Additional Hop

Network sync can be extended by one additional link in any of the following network designs:

> ***NOTE:***
> In each of these following designs, Link 2 *is not* on the same frequency band as Link 4. (For example, Link 2 may be a 5.2-GHz link while Link 4 is a 5.7- or 2.4-GHz link.)

- Design 3
  - A CMM provides sync to a co-located AP.
  - This AP sends the sync over the air to an SM.
  - This SM delivers the sync to a co-located AP.
  - This AP passes the sync in the additional link over the air to SMs.

This design is illustrated in Figure 29.

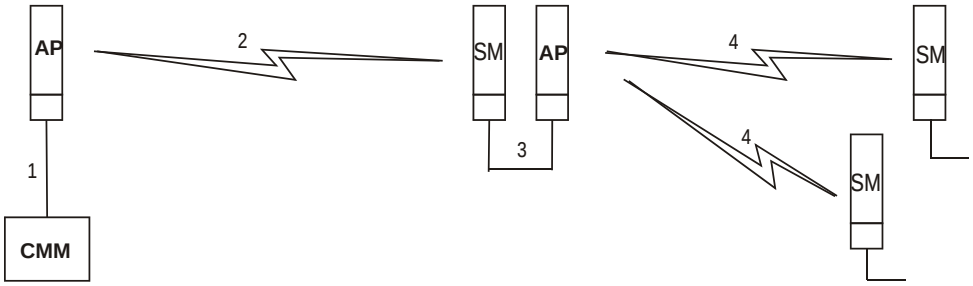


Figure 29: Additional link to extend network sync, Design 3

- Design 4
  - A CMM provides sync to a co-located AP.
  - This AP sends the sync over the air to an SM.
  - This SM delivers the sync to a co-located BHM.
  - This BHM passes the sync in the additional link over the air to a BHS.

This design is illustrated in Figure 30.

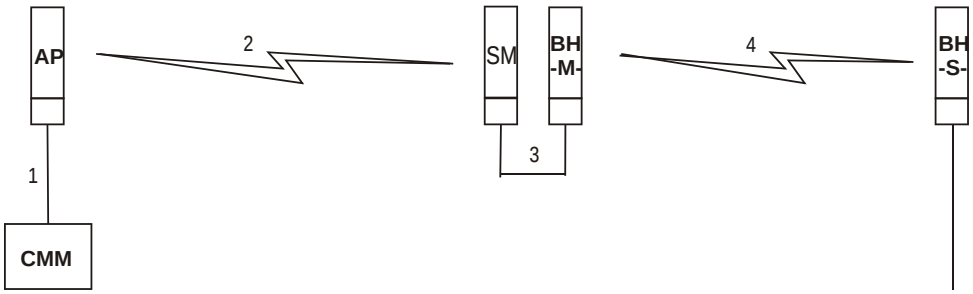


Figure 30: Additional link to extend network sync, Design 4

- Design 5
  - A CMM provides sync to a co-located BHM or the BHM generates timing.
  - This BHM sends the sync over the air to a BHS.
  - This BHS delivers the sync to a co-located AP.
  - This AP passes the sync in the additional link over the air to SMs.

This design is illustrated in Figure 31.

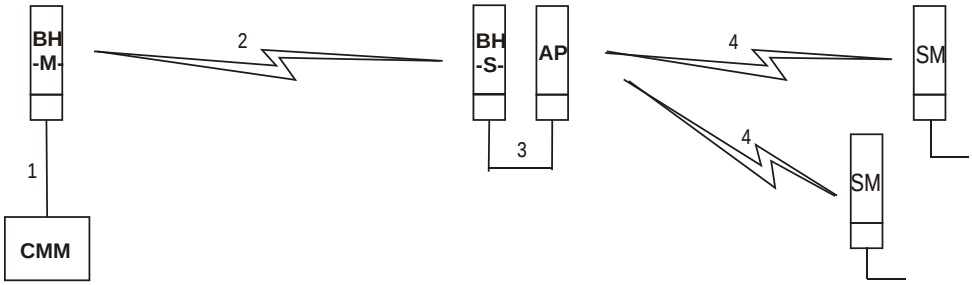


Figure 31: Additional link to extend network sync, Design 5

Wiring and configuration information for this sync extension is described under Wiring to Extend Network Sync on Page 426.

All radios support the remote AP functionality. The BHS and the SM can reliably pass the sync pulse, and the BHM and AP can reliably receive it. The sync is passed in a cable that connects Pins 1 and 6 of the RJ-11 timing ports of the two modules. (The sync cable is described under Cables on Page 57.) When you connect modules in this way, you must also adjust configuration parameters to ensure that

- the AP is set to properly receive sync.
- the SM will not propagate sync to the AP if the SM itself ceases to receive sync.

Chapter 8: Meeting Link Requirements

AP-SM Links

APs communicate with SMs using a point-to-multipoint protocol. An AP-SM link has lower throughput and higher latency than a backhaul link for two reasons:

- Many endpoints are involved.
- The bandwidth request and reservation process consumes bandwidth.

In the 900-MHz frequency band range, round-trip latency is typically 15 msec. In all other frequency band ranges, round-trip latency is typically 6 msec.

At range settings of greater than 40 miles (64 km) in the 900-MHz AP, more time elapses between transmit and receive cycles to compensate for greater air delay. In each frame, this reduces the number of data slots, which slightly reduces the aggregate throughput of the link. However, the throughput is as predictable as in other point-to-multipoint links.

Throughput is a factor of the **Max Range** parameter in the AP and is effective for all SMs, regardless of their distance from the AP. Throughput includes all downlink data to all SMs and all uplink data from all SMs that link to the AP. For throughput, see Table 14 on Page 63.

End user perspective of throughput is based on both bandwidth in the sending direction and the return of TCP acknowledgement packets in the other. Where sufficient downlink bandwidth exists to support downlink traffic and overhead, transient traffic congestion in the uplink can cause some TCP acknowledgement packets to be dropped, and the end user to perceive a reduction in throughput. This can also occur with sufficient uplink bandwidth and dropping acknowledgment packets in the downlink.

However, a network operator can optionally enable the **Prioritize TCP ACK** parameter in the AP and BHM, giving these packets priority over other packet types. This results in fewer of them being dropped.

The effects of changing network conditions on PTMP throughput are indicated in Table 24.

Table 24: Effects of network conditions on PTMP throughput

Changing Network Condition	Effect on AP Aggregate Throughput
Increasing the **Max Range** parameter setting[1] in the AP	somewhat decreased[2]
Increasing the number of SMs that register in the AP	no effect
Increase in downlink traffic	
Increase in uplink traffic	
Increasing the average bandwidth allotted to the SMs that register in the AP	no effect, even when the additional bandwidth is used.

NOTES:

1. For non 900-MHz APs, the AP accepts a **Max Range** value of up to 30 miles (48 km). See Max Range on Page 249.
2. To avoid a decrease of unnecessary proportion, set to not much further than the distance between the AP and the furthest SM that registers in the AP.

A comparison of SM products in link with a CAP 130 is shown in Table 25.

Table 25: Comparison of SM products with CAP 130

Product	Maximum Sustained Aggregate Throughput to a Single SM	Burst	Cap on Committed Information Rate	Upgradability	VoIP Channels Supported
CSM 130	14 Mbps	14 Mb	none	none	multiple
PMP 400 Series SM	21 Mbps	21 Mb	none	none	multiple
CSM 120	7 Mbps	14 Mb	none	to CSM 130 capabilities	multiple
CSM 110 Lite SM as purchased	512 kbps	768 kb	100 kbps	to 1, 2, 4, or 7 Mbps	1
CSM 110 Lite SM upgraded to 1 Mbps	1 Mbps	1.5 Mb	100 kbps	none	1
CSM 110 Lite SM upgraded to 2 Mbps	2 Mbps	3 Mb	100 kbps	none	1
CSM 110 Lite SM upgraded to 4 Mbps	4 Mbps	7 Mb	200 kbps	none	2
CSM 110 Lite SM upgraded to 7 Mbps	7 Mbps	7 Mb	200 kbps	none	2

BH-BH Links

Cambium PTP Bridges communicate with each other using a point-to-point protocol. This point-to-point protocol uses a 2.5-msec frame. A BH link has higher throughput and lower latency (typically 5 msec, 2.5 msec in each direction) for two reasons:

- Only two endpoints are involved.
- No bandwidth request and reservation process is involved.

For 10-Mbps BHs, the aggregate throughput on the channel is 7.5 Mbps. For 20-Mbps BHs, the aggregate throughput on the channel is 14 Mbps. If a BH is set to a downlink ratio of 50%, then the bandwidth in each direction is half of the total BH link bandwidth.

Chapter 9: Previewing Network Configurations

The following are examples of network layouts. Customer experience case studies are also available on the Cambium Networks website:

- http://www.cambiumnetworks.com

Viewing Typical Layouts

The following layouts are typical of system implementations:

- Figure 32: Typical network layout with no BH
- Figure 33: Typical network layout with BH
- Figure 34: Typical multiple-BH network layout

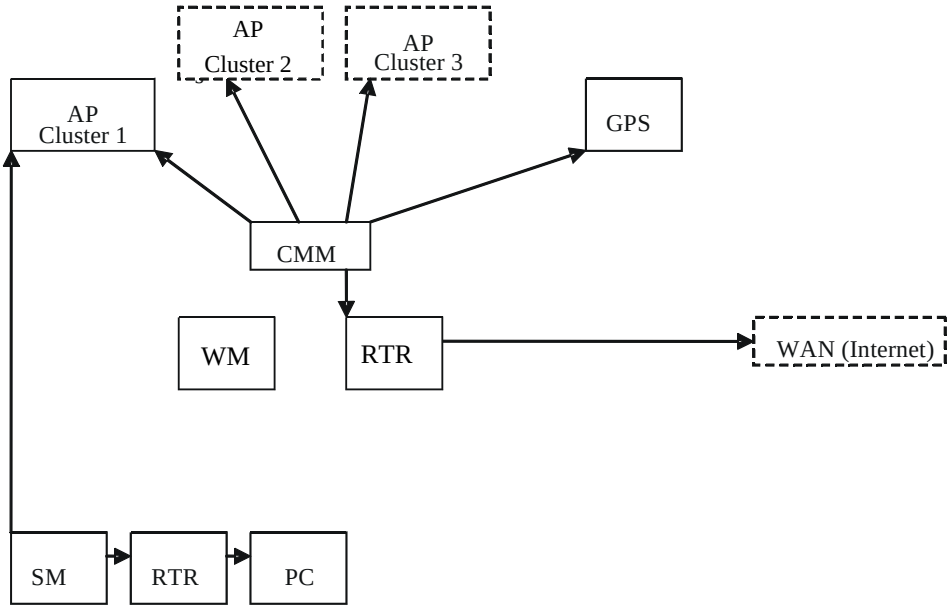


Figure 32: Typical network layout with no BH

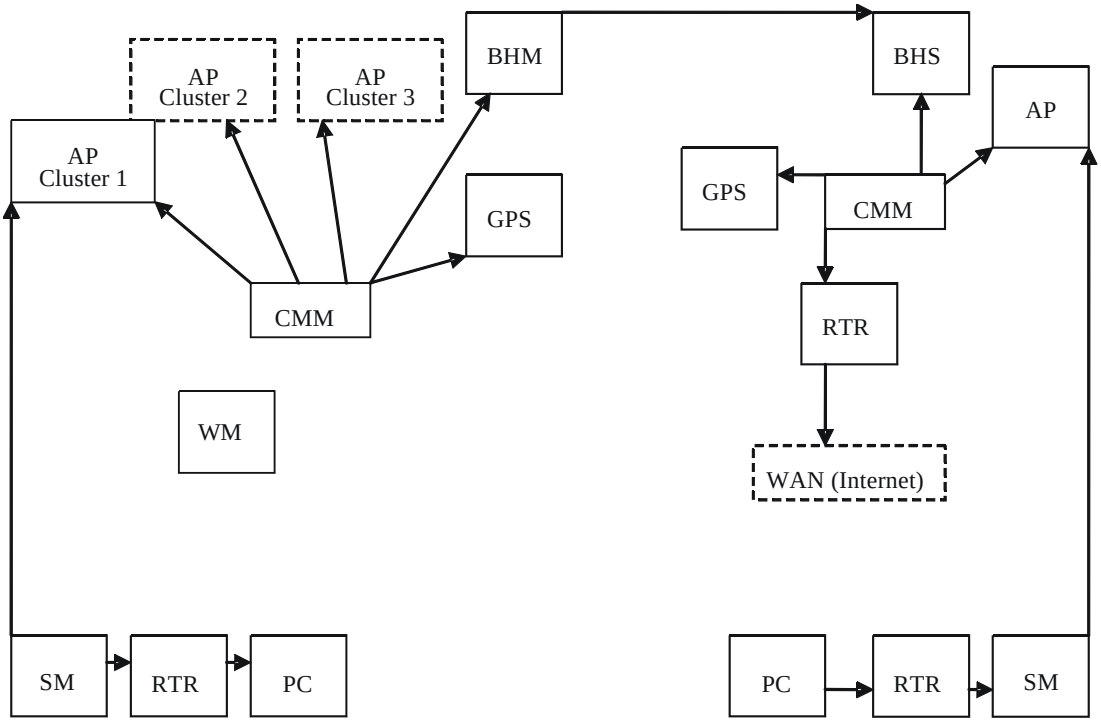


Figure 33: Typical network layout with BH

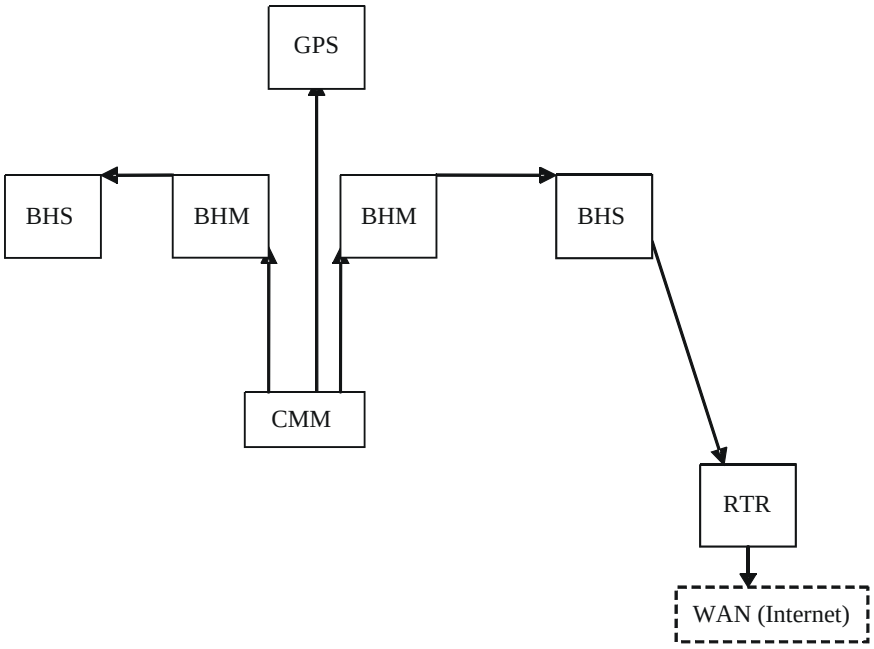


Figure 34: Typical multiple-BH network layout

Chapter 10: Accessing Features

PMP 100 and 400 and PTP 100 and 200 Series radios support the features that are indicated in Table 26.

Table 26: List of features

Regulatory Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
RoHS compliant (EU “green” mandate)	All modules	no	no
WEEE compliant	All modules	no	no
Complies with Human RF exposure limits (ETSI)	All radios	no	no
Radio Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
Time Division Duplex	All radios	no	no
Scalable up to 6 sectors per cell.	AP SM	no	no
200 registered subscribers supported per AP	AP SM	no	no
Fixed/nomadic operation	All radios	no	no
7 ms or less round trip latency (OTA under normal conditions)	All radios	no	no
Transmit frame spreading for geographical area co-existence	AP BHM	Configuration/Radio	yes
Radio statistics (scheduler)	All radios	Statistics/Scheduler	yes
2X rate, enabled per link (requires CAP 130, CAP 09130, or 20 Mbps BH)	SM BHS	Configuration/General	yes
2X rate, enabled per sector (requires CAP 130, CAP 09130, or 20 Mbps BH)	AP BHM	Configuration/General	yes
Manual transmit power control - normal and low (-18 dB)	All radios	Configuration/Radio	yes
Manual transmit power control, 1 dB increments over 25 dB at the AP	AP BHM	Configuration/Radio	yes
SM Transmit Power Control (Automatic SM Transmit Power Adjustment)	AP BHM	Configuration/Radio	yes
SM Receive Target Level	AP BHM	Configuration/Radio	yes

6,200 packets per second on P10 or P11 firmware (6,300 in PMP 400 Series modules without VLAN enabled; 5,300 with VLAN enabled; 6,200 in PTP 100 Series wireless Ethernet bridges at 2- and 4-Mbps throughput; 4,600 in CAP 09130 and CSM 09130)	All radios	no	no
Settable downlink broadcast repeat count	AP	Configuration/Radio	yes
RF Configuration Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
Configurable center-channel carrier frequency	AP BHM	Configuration/Radio	yes
255 configurable, prioritized "color codes" to manage SM to AP (or (BHS to BHM) registration	All radios	Configuration/Radio	yes
16 configurable "sector IDs" for administrative convenience	AP BHM	Configuration/Radio	yes
Configurable range settings (determines air turn-around time)	AP	Configuration/Radio	yes
Configurable downlink data % (determines transmit/receive ratio)	AP BHM	Configuration/Radio	yes
Configurable number of reserved control slots (manages contention for uplink requests)	AP	Configuration/Radio	yes
Configurable frequency scan list at SM	SM BHS	Configuration/Radio	yes
Large Virtual Circuit Data Queue	SM	Configuration/Radio	yes
Packet stats - RF interface	All radios	Statistics/Radio	yes
Installation Color Code	AP BHM	Configuration / Radio	yes
Timing Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
Configurable AP/BHM sync source - Sync over Power over Ethernet, self-sync, or sync cable	AP BHM	Configuration/General	yes
"Remote AP" support, including timing pulse propagation through SM/BHS	SM BHS	Configuration/General	yes

Ethernet Interface Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Selectable link speeds - 10/100 Base T, half, full-duplex	All modules	Configuration/General	yes
Ethernet link auto-negotiation	All modules	Configuration/General	no
Accepts straight-through or crossover Ethernet cable wiring (Auto-MDX)	All modules	no	no
Wire line Interface: Ethernet cable with proprietary PoE	All modules	no	no
Disable SM Ethernet link	SM	Configuration/General	yes
Packet stats - Ethernet interface	All radios	Statistics/Ethernet	Yes
IP Interface Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
Configurable LAN settings (IP address, mask, gateway)	All radios	Configuration/IP	yes
Module's management IP address assignable via DHCP	All radios	Configuration/IP	yes
DHCP Relay Agent	AP	Configuration/General	yes
Private LAN to support AP to SM (or BHM to BHS) communications	All radios	Configuration/IP	yes
DNS Server / Domain Name configuration	All radios	Configuration/IP	yes
Configurable SM mgmt accessibility (Local/Ethernet only, or Public/RF and Local/Ethernet)	SM	Configuration/IP	yes

Security Features (Authentication, Encryption, and Access Control)	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Configurable SM authentication using BAM/PrizmEMS/RADIUS	AP SM	Configuration/Security	yes
Configurable BH authentication, standalone	BHM BHS	Configuration/Security	no
DES encryption on standard product	All radios	no	yes
AES encryption on AES product	All radios	no	yes
Configurable whether SM/BHS displays AP/BHM beacon information	AP BHM	Configuration/Security	yes
Configurable web, telnet, and ftp session timeout	All radios	Configuration/Security	yes
Configurable access to radio management - up to 3 source IP addresses	All radios	Configuration/Security	yes
User/account names (up to 4) and passwords on modules	All radios	Account	yes
Permission levels control ability to add/delete users/passwords	All radios	Account	yes
Override plug to override lost IP address or user/password	All radios	no	no
Override plug configurable as a default plug - reset to factory defaults	AP SM BHM BHS	Configuration/Unit Settings	yes
Override switch to override lost IP address or user/password on CMM	CMMmicro CMM4	no	no
Capability to disable refresh of the encryption key every 24 hours	BHM	Configuration/Security	yes
RF Telnet Control	AP	Configuration/Security	yes
Read only community string configurable	AP	Configuration/SNMP	yes

Monitoring Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
List of registered SMs/BHSs with full data, with hot links to SMs/BHSs	AP BHM	Configuration/General	multiple objects
Abbreviated list of SMs/BHSs, with hot links to SMs/BHSs	AP BHM	Configuration/General	multiple objects
Received power level indication	All radios	Home/Session Status (in master)	yes
LEDs on modules to display states and activity	All modules	no	no
Received interference level indication (jitter)	All radios	Configuration/General	yes
Configurable web-page auto-refresh	All modules	Configuration/General	yes
SM registration failures	AP BHM	Statistics/Reg Failures	yes
Event log	All modules	Home/Event Log	no
Operator can use own logo on GUI pages	All modules	no	yes
Operator can use own style sheets for GUI	All modules	no	yes
Jitter consistent regardless of operation (1X or 2X)	All radios	no	no
Link status table with bidirectional data for all links	AP	Tools/Link Status	no
Point-to-Point Protocol over Ethernet (PPPoE) client	SM	Configuration/PPPoE	yes
Maximum number of SMs registered since last reboot displayed	AP	Home/General Status	no
Overload statistics	AP	Statistics/Scheduler	
Per-SM query (instead of Link Status table)	AP	Tools/Link Status	no
Bridge Management Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
Configurable bridge entry timeout	All radios	Configuration/General	yes
Bridging table statistics (up to 4096 entries)	All radios	Statistics/Bridging Table	yes
Disable bridging on BHs	BHM BHS	Configuration/General	yes
SM Isolation Features (preventing communication between SMs)	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
SM isolation at AP	AP	Configuration/General	yes
SM isolation at CMM	CMMmicro CMM4	Configuration/General	yes

SM Isolation Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Translation bridging (replace customer MAC with SM MAC address)	AP	Configuration/General	yes
With Translation bridging, choice of sending untranslated ARP	AP	Configuration/General	yes
Translation table statistics	All radios	Statistics/Translation Table	yes
Quick Start Feature	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
AP configuration quick-start wizard	AP BHM	Quick Start	
Bandwidth Management Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
AP Maximum Information Rate (MIR) default settings	AP	Configuration/QoS	yes
Per SM Maximum Information Rate (MIR)	SM	Configuration/QoS	yes
Per SM Committed Information Rate (CIR) for high and low channels	SM	Configuration/QoS	yes
"Configuration Source" for MIR/CIR/HP/VLAN can be either SM or BAM/Prizm/RADIUS	AP	Configuration/General	yes
CIR for low priority channel on BH	BHS	Configuration/QoS	yes
Configurable priority for TCP Acks, to optimize bandwidth use	AP BHM	Configuration/General	yes
Settable broadcast downlink CIR	AP	Configuration/QoS	yes
Bandwidth Management Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
Configurable High Priority channel with configurable DiffServ mappings on AP, SM (2 classes of service)	AP SM	Configuration/Diffserv	yes
Permanent BH High Priority Channel with configurable DiffServ mappings on BH (2 classes of service)	BHM BHS	Configuration/Diffserv	yes
Virtual channel (high/low priority) statistics	All radios	Statistics/Data VC	yes

Network Address Translation (NAT) Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
NAT	SM	Configuration/NAT	yes
NAT DMZ	SM	Configuration/NAT	yes
NAT DHCP server on LAN with up to 254 IP addresses in pool	SM	Configuration/NAT	yes
NAT DHCP client on WAN (obtains NAT address from a DHCP server)	SM	Configuration/NAT	yes
NAT port mapping	SM	Configuration/NAT	yes
VPN "pass through" for L2TP over IPSec (but not PPTP)	SM	no	no
NAT statistics	SM	Statistics/NAT Stats	yes
NAT DHCP statistics	SM	Statistics/NAT DHCP Statistics	yes
NAT table	SM	Logs/NAT Table	no
Filtering Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
Protocol filtering based on protocol	All radios	Configuration/Protocol Filtering	yes
Operator-defined port filtering (3 ports)	All radios	Configuration/Protocol Filtering	yes
DNS Server Proxy	SM	Configuration/NAT	yes
Packet filter statistics	All radios	Statistics/Filter	yes
VLAN Management Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
Configurable VLAN	AP SM CMMmicro CMM4	Configuration/VLAN	yes
Highly configurable VLAN (802.1Q)	AP SM	Configuration/VLAN	yes
Use of VLAN priorities (802.1p) with high priority channel	AP SM	no	yes
Q-in-Q VLAN Tagging	All radios	Configuration/VLAN	yes
Port-based VLAN switching on CMM	CMMmicro CMM4	Configuration	yes
VLAN statistics	AP SM	Statistics/VLAN	yes
Dynamic Frequency Selection (DFS) Feature	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
DFS v1.2.3	All radios	no	yes
DFS v1.3.1	All radios	no	yes
DFS v1.4.1	All radios	no	yes

Time Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Time and Date from CMM via Network Time Protocol (NTP) server	AP BHM	Configuration/Time	yes
Time and Date manually settable	AP BHM	Configuration/Time	yes
CMM provides NTP server	CMMmicro CMM4	no	no
Spectrum Analyzer Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
Spectrum analyzer	SM BHS	Tools/Spectrum Analyzer	no
Ability to switch an AP to an SM (or BHS to BHM)	AP BHM	Configuration/General	yes
Remote Spectrum Analysis	AP	Tools/Remote Spectrum Analyzer	no
Aim/Link Quality Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
Alignment tone for using during aiming/alignment	SM BHS	no	no
Aiming support page when not using alignment tone	SM BHS	Tools/Alignment	multiple objects
LED for alignment	SM BHS	no	no
Configure SM power-up state - aiming or operational	SM BHS	Configuration/General	yes
Link capacity test, with configurable packet length	All radios	Tools/Link Capacity Test	yes
Display of SM configuration information at AP	AP BHM	Home/Session Status	yes
Display/evaluation of AP beacon data from all receivable APs	SM BHS	Tools/AP Evaluation	yes
Over-the-air radio Bit Error Rate (BER) indicator	SM	Tools/BER Results	yes
Graphical alignment tool with near-real time jitter and received power level	SM	Tools/Alignment Tool	no
Optional selection of Revised or Legacy LED indicator scheme	SM	Configuration/Unit Settings	no
Frame Tool Feature	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
Frame calculator for supporting co-location	All radios	Tools/Frame Calculator	no

Personal Digital Assistant (PDA) Interface Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
GUI automatically sized/styled for PDA when displayed on a PDA	All radios	all	no
Spectrum analyzer display for PDA	All radios	PDA/Spectrum Results (PDA)	no
Specific pages for PDA display	All radios	PDA	no
SNMP Interface Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
Support of SNMP v2	All modules	no	no
Canopy Enterprise MIB	All modules	no	no
Configurable SNMP community string	All radios	Configuration/SNMP	yes
Configurable SNMP accessing subnet	All radios	Configuration/SNMP	yes
10 configurable SNMP trap addresses	All radios	Configuration/SNMP	yes
Configurable traps (sync and session)	All radios	Configuration/SNMP	yes
Configurable SNMP permissions (read, read/write)	All radios	Configuration/SNMP	yes
Configurable site information, including site name	All modules	Configuration/SNMP	yes
Upgrade Process Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
Upgrading using CNUT and SM Auto-update for SMs	All modules	no	no
Configurable update address to support distributed software upgrades	AP	Configuration/General	yes
AP Cluster Management Features	**Module Type(s)**	**Controlled in GUI Page/Tab**	**SNMP Control**
CMM port power control	CMMmicro CMM4	Configuration	yes
CMM port reset	CMMmicro CMM4	Configuration	yes
CMM: Sufficient ports for at least 4 AP, 2 BH, plus management	CMMmicro CMM4	no	no
CMM: Sufficient power for at least 4 AP plus 2 BH	CMMmicro CMM4	no	no
Powered from 90-264 VAC, 50/60 Hz; 55 V DC power output	AP BH	no	no

Physical Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
MTBF > 45 years (~400 000 hours)	All modules	no	no
neg 40 C to + 55 C (Ambient) operation	All modules	no	no
Temperature indication	All radios	Home/General	no
Non-condensing (Indoor/outdoor), weather protected form factor/packaging	All modules	no	no

Activating Features

A feature is *active* if the software that allows the feature to be turned on or off (enabled or disabled) is present.

Fixed License Keys

Some features are activated by loading a fixed license key into the radio. Such a key arrives from Cambium as a *filename*.url file. When you double-click on this file, your browser opens and the location bar is populated by a lengthy string. This URL string begins with http://<ModuleIPAddress>. If you need to load a key into a module whose IP address has changed since Cambium issued the key, perform the following steps.

Procedure 1: Modifying a fixed license key for a module IP address

1. Right-click on the license key filename.
2. Select **Properties**.
3. Select the **Web Document** tab.
4. At **URL**, substitute the current IP address for the original IP address in the URL.
5. Click **OK**.
6. Double-click on the license key filename.
   RESULT: The key loads into the module.
7. Open the Configuration web page of the module.
8. Review parameter settings and enable the feature if you wish to do so at this time (see next section).

Enabling Features

A feature is *enabled* (functioning) if the feature is both active and enabled. For example, Transmit Frame Spreading is active (*can be* enabled) in any AP or BHM, except 900-MHz radios. However, Transmit Frame Spreading functions only if the **Enable** selection for the **Transmit Frame Spreading** parameter is checked in the Radio tab of the Configuration web page in the module.

Chapter 11: Acquiring Proficiencies

Designing and operating a network requires fundamental knowledge of radio frequency transmission and reception, Internet Protocol addressing schemes, experimentation with equipment, and for most operators participation in some forms of product training.

Understanding RF Fundamentals

Product training and user interfaces presume an understanding of RF fundamentals. Excellent written sources for these fundamentals are available. One such source is *Deploying License-Free Wireless Wide-Area Networks* by Jack Unger (ISBN 1-58705-069-2), published by Cisco Press.

Understanding IP Fundamentals

Product training and user interfaces also presume an understanding of Internet Protocol (IP) fundamentals. Excellent written sources for these fundamentals are available. One such source is *Sams Teach Yourself TCP/IP in 24 Hours* by Joe Casad
(ISBN 0-672-32085-1), published by Sams Publishing.

NOTE:
The default IP address of each component is 169.254.1.1.

Acquiring a Demonstration Kit

Demonstration Kits are available through your Cambium representative.

900-MHz with Integrated Antenna and Band-pass Filter Demonstration Kit

Each 900-MHz with integrated antenna and band-pass filter Demonstration Kit contains

- 2 9000SM SMs
- 1 9000APF AP
- 1 600SS Surge Suppressor
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 UGTK-0002 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD03EN Technical Overview on CD
- 1 User Guide on CD

Part numbers for Demonstration Kits are provided in Table 27.

900-MHz with Connectorized Antenna Demonstration Kit

Each 900-MHz with connectorized (external) antenna Demonstration Kit contains

- 2 9000SMC CSM 09130s
- 1 9000APC CAP 09130
- 3 AN900 60° 9-dBi Antennas
- 1 600SS Surge Suppressor
- 1 SMMB2 Universal Heavy Duty Mounting Bracket
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 UGTK-0002 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD03EN Technical Overview on CD
- 1 User Guide on CD

Part numbers for Demonstration Kits are provided in Table 27.

2.4-GHz with Adjustable Power Set to High Demonstration Kit

Each 2.4-GHz with adjustable power set to high Demonstration Kit contains

- 1 2400SM SM
- 1 2450SM CSM 130
- 1 2450AP CAP 130
- 1 600SS Surge Suppressor
- 1 SMMB1 Universal Mounting Bracket
- 3 ACPSSW-02 90- to 230-V AC 50- to 60-Hz Power Supplies
- 1 UGTK-0002 Trial Kit Quick Start Guide

- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD03EN Technical Overview on CD
- 1 User Guide on CD

Part numbers for Demonstration Kits are provided in Table 27.

5.2-GHz Demonstration Kit

Each 5.2-GHz Demonstration Kit contains

- 1 5200SM SM
- 1 5250SM CSM 130
- 1 5250AP CAP 130
- 1 600SS Surge Suppressor
- 1 SMMB1 Universal Mounting Bracket
- 3 ACPSSW-02 90- to 230-V AC 50- to 60-Hz Power Supplies
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 UGTK-0002 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD03EN Technical Overview on CD
- 1 User Guide on CD

Part numbers for Demonstration Kits are provided in Table 27.

5.4-GHz Demonstration Kit

Each 5.4-GHz Demonstration Kit contains

- 1 5400SM SM
- 1 5450SM CSM 130
- 1 5450AP CAP 130
- 1 600SS Surge Suppressor
- 1 SMMB1 Universal Mounting Bracket
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 Cross-over Category 5 Cable
- 1 UGTK-0002 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD03EN Technical Overview on CD
- 1 User Guide on CD

Part numbers for Demonstration Kits are provided in Table 27.

5.7-GHz with Connectorized Antenna and Adjustable Power Set to Low Demonstration Kit

Each 5.7-GHz with connectorized antenna and adjustable power set to low Demonstration Kit contains

- 1 5700SMC SM
- 1 5750SMC CSM 130
- 1 5750APC CAP 130
- 1 600SS Surge Suppressor
- 1 SMMB2 Universal Heavy Duty Mounting Bracket
- 3 ACPSSW-02 90- to 230-V AC 50- to 60-Hz Power Supplies
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 Cross-over Category 5 Cable
- 1 UGTK-0002 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD03EN Technical Overview on CD
- 1 User Guide on CD

Part numbers for Demonstration Kits are provided in Table 27.

Demonstration Kit Part Numbers

The part numbers for ordering demonstration kits are provided in Table 27.

Table 27: Demonstration Kit part numbers

Frequency Band Range and Feature	Current Part Number	Previous Part Number
900 MHz integrated antenna with band-pass filter	HK1267B	TK10290
900 MHz connectorized antenna	HK1244B	TK10290C
2.4 GHz adjustable power set to low		TK10250
2.4 GHz adjustable power set to high	HK1135B	TK10251
5.2 GHz	HK1133B	TK10252
5.4 GHz	HK1282A	TK10254
5.7 GHz		TK10257
5.7 GHz connectorized adjustable power set to low	HK1132B	TK10257C

Acquiring a Starter Kit

Starter Kits are also available through your Cambium representative.

900-MHz with Integrated Antenna and Band-pass Filter Starter Kit

Each 900-MHz with integrated antenna and band-pass filters Starter Kit contains

- 20 9000SM CSM 09130s
- 3 9000APF CAP 09130s
- 1 1070CK CMMmicro
- 21 600SS Surge Suppressors
- 1 User Guide on CD

Power supplies and SM mounting brackets are not included in this kit. Part numbers for Starter Kits are provided in Table 28.

900-MHz with Connectorized Antenna Starter Kit

Each 900-MHz with connectorized (external) antenna Starter Kit contains

- 20 9000SMC CSM 09130s
- 3 9000APC CAP 09130s
- 1 1070CK CMMmicro
- 21 600SS Surge Suppressors
- 20 SMMB2 Universal Heavy Duty Mounting Brackets
- 1 User Guide on CD

Power supplies *are not* included in this kit. Part numbers for Starter Kits are provided in Table 28.

2.4-GHz with Adjustable Power Set to High Starter Kit

Each 2.4-GHz adjustable power set to high Starter Kit contains

- 30 2400SM CSM 120s
- 6 2450AP CAP 130s
- 1 1070CK CMMmicro
- 31 600SS Surge Suppressors
- 30 SMMB1 Universal Mounting Brackets
- 1 User Guide on CD

Power supplies *are not* included in this kit. Part numbers for Starter Kits are provided in Table 28.

5.2-GHz Starter Kit

Each 5.2-GHz Starter Kit contains

- 30 5200SM CSM 120s
- 6 5250AP CAP 130s
- 1 1070CK CMMmicro
- 31 600SS Surge Suppressors
- 30 SMMB1 Universal Mounting Brackets
- 1 User Guide on CD

Power supplies *are not* included in this kit. Part numbers for Starter Kits are provided in Table 28.

5.4-GHz FSK Starter Kit

Each 5.4-GHz Starter Kit contains

- 30 5400SM CSM 120s
- 6 5450AP CAP 130s
- 1 1070CK CMMmicro
- 31 600SS Surge Suppressors
- 30 SMMB1 Universal Mounting Brackets
- 1 User Guide on CD

Power supplies *are not* included in this kit. Part numbers for Starter Kits are provided in Table 28.

5.4-GHz OFDM Starter Kits

Starter kits for PMP 54400 series network equipment are available in three sizes. Each HK1820A Starter Kit contains

- 2 5440 SMs
- 1 5440 AP
- 3 ACPSSW-13B Power Supplies
- 3 600SS Surge Suppressors
- 2 SMMB2A Mounting Brackets

Each HK1819A Starter Kit contains

- 5 5440 SMs
- 2 5440 APs
- 6 ACPSSW-13B Power Supplies
- 6 600SS Surge Suppressors
- 5 SMMB2A Mounting Brackets

Each HK1818A Starter Kit contains

- 20 5440 SMs
- 2 5440 APs
- 20 ACPSSW-13B Power Supplies
- 22 600SS Surge Suppressors
- 20 SMMB2A Mounting Brackets

Part numbers for Starter Kits are provided in Table 28.

5.7-GHz with Integrated Antenna Starter Kit

Each 5.7-GHz with integrated antenna Starter Kit contains

- 30 5700SM CSM 120s
- 6 5750AP CAP 130s
- 1 1070CK CMMmicro
- 31 600SS Surge Suppressors
- 30 SMMB1 Universal Mounting Brackets
- 1 User Guide on CD

Power supplies *are not* included in this kit. Part numbers for Starter Kits are provided in Table 28.

Starter Kit Part Numbers

The part numbers for ordering Starter kits are provided in Table 28.

Table 28: Starter Kit part numbers

Frequency Band Range	Current Part Number	Previous Part Number
900 MHz integrated antenna with band-pass filter	HK1266B	TK10190
900 MHz connectorized	HK1243B	TK10190C
2.4 GHz adjustable power set to low		TK10150
2.4 GHz adjustable power set to high	HK1139B	TK10151
5.2 GHz	HK1140B	TK10152
5.4 GHz FSK	HK1283A	TK10154
5.4 GHz OFDM	HK1118A	
	HK1119A	
	HK1120A	
5.7 GHz	HK1141B	TK10157
5.7 GHz connectorized adjustable power set to low		TK10157C

Chapter 12: Engineering Your RF Communications

Before diagramming network layouts, the wise course is to

- anticipate the correct amount of signal loss for your fade margin calculation (as defined below).
- recognize all permanent and transient RF signals in the environment.
- identify obstructions to line of sight reception.

Anticipating RF Signal Loss

The C/I (Carrier-to-Interference) ratio defines the strength of the intended signal relative to the collective strength of all other signals. Standard modules typically do not require a C/I ratio greater than

- 3 dB or less at 10-Mbps modulation and −65 dBm for 1X operation. The C/I ratio that you achieve must be even greater as the received power approaches the nominal sensitivity (−85 dBm for 1X operation).
- 10 dB or less at 10-Mbps modulation and −65 dBm for 2X operation. The C/I ratio that you achieve must be even greater as the received power approaches the nominal sensitivity (−79 dBm for 2X operation).
- 10 dB or less at 20-Mbps modulation.

Nominal receive sensitivity in PMP 400 Series modules is as follows:

- −89 dBm for 1X operation
- −78 dBm for 2X operation
- −70 dBm for 3X operation

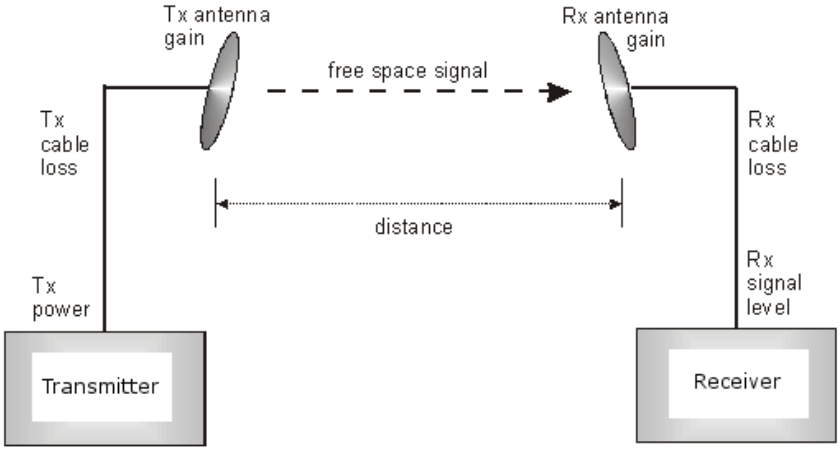
Understanding Attenuation

An RF signal in space is attenuated by atmospheric and other effects as a function of the distance from the initial transmission point. The further a reception point is placed from the transmission point, the weaker is the received RF signal.

Calculating Rx Signal Level

The Rx sensitivity of each module is provided at http://www.cambiumnetworks.com. The determinants in Rx signal level are illustrated in Figure 35.

Figure 35: Determinants in Rx signal level



Rx signal level is calculated as follows:

Rx signal level dB = *Tx power* − *Tx cable loss* + *Tx antenna gain* − *free space path loss* + *Rx antenna gain* − *Rx cable loss*

NOTE:
This Rx signal level calculation presumes that a clear line of sight is established between the transmitter and receiver and that no objects encroach in the Fresnel zone.

Calculating Fade Margin

Free space path loss is a major determinant in Rx (received) signal level. Rx signal level, in turn, is a major factor in the system operating margin (fade margin), which is calculated as follows:

system operating margin (fade margin) dB =Rx signal level dB − Rx sensitivity dB

Thus, fade margin is the difference between strength of the received signal and the strength that the receiver requires for maintaining a reliable link. A higher fade margin is characteristic of a more reliable link.

Analyzing the RF Environment

An essential element in RF network planning is the analysis of spectrum usage and the strength of the signals that occupy the spectrum you are planning to use. Regardless of how you measure and log or chart the results you find (through the Spectrum Analyzer in SM and BHS feature or by using a spectrum analyzer), you should do so

- at various times of day.
- on various days of the week.
- periodically into the future.

As new RF neighbors move in or consumer devices in your spectrum proliferate, this will keep you aware of the dynamic possibilities for interference with your network.

Mapping RF Neighbor Frequencies

These modules allow you to

- use an SM or BHS (or a BHM reset to a BHS), or an AP that is temporarily transformed into an SM, as a spectrum analyzer.
- view a graphical display that shows power level in RSSI and dBm at 5-MHz increments throughout the frequency band range, regardless of limited selections in the **Custom Radio Frequency Scan Selection List** parameter of the SM.
- select an AP channel that minimizes interference from other RF equipment.

The SM measures only the spectrum of its manufacture. So if, for example, you wish to analyze an area for both 2.4- and 5.7-GHz activity, take both a 2.4- and 5.7-GHz SM to the area. To enable this functionality, perform the following steps:

CAUTION!

The following procedure causes the SM to drop any active RF link. If a link is dropped when the spectrum analysis begins, the link can be re-established when either a 15-minute interval has elapsed or the spectrum analyzer feature is disabled.

Procedure 2: Analyzing the spectrum

1. Predetermine a power source and interface that will work for the SM or BHS in the area you want to analyze.
2. Take the SM or BHS, power source, and interface device to the area.

3. Access the Tools web page of the SM or BHS.
   RESULT: The Tools page opens to its Spectrum Analyzer tab. An example of this tab is shown in Figure 146.
4. Click **Enable**.
   RESULT: The feature is enabled.
5. Click **Enable** again.
   RESULT: The system measures RSSI and dBm for each frequency in the spectrum.
6. Travel to another location in the area.
7. Click **Enable** again.
   RESULT: The system provides a new measurement of RSSI and dBm for each frequency in the spectrum.
   NOTE: Spectrum analysis mode times out 15 minutes after the mode was invoked.
8. Repeat Steps 6 and 7 until the area has been adequately scanned and logged.

As with any other data that pertains to your business, a decision today to put the data into a retrievable database may grow in value to you over time.

RECOMMENDATION:
Wherever you find the measured noise level is greater than the sensitivity of the radio that you plan to deploy, use the noise level (rather than the link budget) for your link feasibility calculations.

Anticipating Reflection of Radio Waves

In the signal path, any object that is larger than the wavelength of the signal can reflect the signal. Such an object can even be the surface of the earth or of a river, bay, or lake. The wavelength of the signal is approximately

- 2 inches for 5.2- and 5.7-GHz signals.
- 5 inches for 2.4-GHz signals.
- 12 inches for 900-MHz signals.

A reflected signal can arrive at the antenna of the receiver later than the non-reflected signal arrives. These two or more signals cause the condition known as multipath. Multipath may increase or decrease the signal level and so overall attenuation may be higher or lower than that caused by the link distance. This is problematic at the margin of the link budget, where the standard operating margin (fade margin) may be compromised.

Noting Possible Obstructions in the Fresnel Zone

The Fresnel (pronounced *fre·NEL*) Zone is a three-dimensional volume around the line of sight of an antenna transmission. Objects that penetrate this area can cause the received strength of the transmitted signal to fade. Out-of-phase reflections and absorption of the signal result in signal cancellation.

The foliage of trees and plants in the Fresnel Zone can cause signal loss. Seasonal density, moisture content of the foliage, and other factors such as wind may change the amount of loss. Plan to perform frequent and regular link tests if you must transmit though foliage.

.

Radar Signature Detection and Shutdown

With Release 8.1, Cambium met *ETSI EN 301 893 v1.2.3* for Dynamic Frequency Selection (DFS) in slave as well as master radios. DFS is a requirement in certain countries and regions for systems to detect interference from other systems, notably radar systems, and to avoid co-channel operation with these systems. With Release 8.1, all 5.7-GHz connectorized modules and all 5.4-GHz modules were ETSI DFS capable. These two products were sold only outside the U.S.A. and Canada. No other products had a DFS option.

The Configuration => Radio web page in Release 8.1 allowed the operator to enable or disable DFS. Operators in countries with regulatory requirements for DFS *must not* disable the feature and *must* ensure that it is enabled after a module is reset to factory defaults. Operators in countries without regulatory requirements for DFS should disable DFS to avoid the additional minute of connection time for APs, BHMs, and SMs, and avoid the additional two minutes for BHSs.

With Release 8.2 and later, all of the 5.2-, 5.4-, and 5.7-GHz master and slave radios satisfy the requirements that the *FCC Report and Order 03-287*, Industry Canada, and *ETSI EN 301 893 v1.3.1* impose for DFS. These regulations differ on

- which radio frequency band(s) have DFS required.
- whether older radios must have DFS enabled.
- whether SMs and BHSs, in addition to APs and BHMs, must have DFS enabled.

Moreover in Release 8.2 and later, 5.4-GHz radios that are set for Canada or Australia omit center channel frequencies from 5580 to 5670 MHz, inclusive, from their GUIs and cannot operate in that range. This satisfies Canadian and Australian requirements that protect weather radio from interference by co-channel operation. This leaves 6 instead of 9 channels at 25-MHz center spacing[3] (or 7 instead of 11 at 20-MHz center spacing). Operators in the U.S.A. should avoid the weather channels as well, but may be able to temporarily use them after spectrum analysis reveals that no competition exists.

[3] 25-MHz center channel spacing is recommended for CAP 130 (Advantage AP) and 20-Mbps BH.

The master radios properly implement the regionally-imposed DFS conditions after reading the value of the **Region Code** parameter, which Release 8.2 introduced. The effect of the DFS feature, based on the **Region Code** value (if this parameter is present), is shown in Table 29.

Table 29: Effect of DFS feature

Region Code[1] Value	Effect of DFS Feature							
	900 MHz	2.4 GHz	5.2 GHz		5.4 GHz		5.7 GHz	
	AP SM	AP SM BH	AP BHM	SM BHS	AP BHM	SM BHS	AP BHM	SM BHS
Australia	No effect	No effect			FCC/IC DFS with notch[2]	No effect	No effect	No effect
Brazil					ETSI DFS	ETSI DFS	No effect	No effect
Canada	No effect	No effect	FCC/IC DFS[3]	No effect	FCC/IC DFS with notch[2]	No effect	No effect	No effect
Europe		No effect			ETSI DFS	ETSI DFS	ETSI DFS	ETSI DFS
Russia			No effect	No effect			No effect	No effect
United States	No effect	No effect	FCC/IC DFS[3]	No effect	FCC/IC DFS	No effect	No effect	No effect
Other	No effect on radio operation							
None	AP or BHM will not transmit							

NOTES:

1. In all cases, set the **Region Code** parameter to the appropriate region. Then the software will determine the correct use of DFS.
2. Center channel frequencies from 5580 to 5670 MHz, inclusive, are omitted (notched out of the otherwise continuous band) from the GUIs and these radios cannot operate in that range.
3. Newly manufactured P10 5.2-GHz radios use DFS. Radios that were purchased without DFS are not required to use DFS.

When an AP or BHM boots, it performs a channel availability check (CAC) for one minute on its main carrier frequency, without transmitting, as it monitors the channel for radar. If it detects no radar signature during this minute, the radio then proceeds to normal beacon transmit mode. If it does detect a radar signature, it locks that frequency carrier out for 30 minutes, and switches to the **Alternate Frequency Carrier 1**, which is set in the Configuration => Radio web page.

For the next minute, the radio monitors this new frequency for radar and, if it detects no radar, it proceeds to beacon transmit mode. If it does detect radar, it locks that frequency carrier out for 30 minutes, and switches to **Alternate Frequency Carrier 2**. For the minute that follows, the radio monitors this second alternate frequency and responds as described above to the presence or absence of radar on its current channel, switching if necessary to the next channel in line.

The ETSI EN 301 893 v1.3.1 specification requires DFS on a slave radio (SM or BHS) also. A slave radio transmits only if it receives a beacon from the master radio (AP or BHM). When the slave radio with DFS boots, it scans to distinguish whether a master radio beacon is present. If it finds a master, the slave

receives on that frequency for one minute without transmitting, as it monitors for a radar signature. Then the slave proceeds as follows:

- If an SM detects no radar during this minute, it attempts to register in the AP. If it does detect radar, it locks out that frequency for 30 minutes and continues scanning other frequencies in its scan list.
- If a BHS detects no radar during this minute, it registers in the BHM. While registering and ranging, it continues *for another full minute* to scan for radar. If it detects radar, it locks out that frequency for 30 minutes and continues scanning other frequencies in its scan list.

The possibility exists for a slave to attempt to register in a different master at this point and to even succeed. This would depend on both of the following conditions:

- matching color code values in the slave and master
- matching transmission frequency of the master to one that the slave is set in the scan list of the slave.

The slave automatically inherits the DFS type of the master. This behavior ignores the value of the **Region Code** parameter in the slave, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), the operator should always set the value that corresponds to the local region.

The Home => General Status web page in any module with DFS displays one of the following status statements in its read-only field **DFS** field under Device Information:

- `Normal Transmit`
- `Radar Detected Stop Transmitting for` *n* `minutes`, where *n* counts down from 30 to 1.
- `Checking Channel Availability Remaining time` *n* `seconds`, where *n* counts down from 60 to 1.
- `Idle`, which indicates that the slave radio is scanning but has failed to detect a beacon from a master radio. When it has detected a beacon, the slave initiates a channel availability check (CAC) on that frequency.

RECOMMENDATION:
Where regulations require that radar sensing and radio shutdown is enabled, you can most effectively share the spectrum with satellite services if you perform spectrum analysis and select channels that are distributed evenly across the frequency band range.

A connectorized 5.7-GHz module provides an **Antenna Gain** parameter. When you indicate the gain of your antenna in this field, the algorithm calculates the appropriate sensitivity to radar signals, and this reduces the occurrence of false positives (wherever the antenna gain is less than the maximum).

Release 9 introduces support for Dynamic Frequency Selection (DFS) ETSI v1.4.1.

A 5.2-, 5.4-, or 5.7-GHz P10 or higher AP or BH with a Region Code set to United States and upgraded to Release 9.5 will continue to be set to the United States Region Code and will not be configurable to another Region Code by installers or end users. As discussed in section 2.3, this is in response to FCC KDB 594280 and ensures that end users and professional installers will not have access to settings which could allow a radio to be configured to operate in a manner other than that which was specified in the FCC equipment authorization grant. After upgrade, the AP or BH will display the Region Code on the Configuration => General page as United States in a gray font, and the parameter is no longer settable.

To prevent co-channel operation with Terminal Doppler Weather Radar (TDWR) systems, P10 and P11 5.4-GHz APs and BHMs configured with a Region Code of United States running Release 9.5 or later will not use or allow configuration of the center channel frequencies shown in Table 30.

Table 30: United States Region Code – unavailble center channels

Product Family	Center Channel Frequencies not Available
FSK – 5.4 GHz	5590 through 5660 MHz (on 5-MHz increments) not available
OFDM – 5.4 GHz	5600 through 5650 MHz (on 5-MHz increments) not available

This applies to the **Radio Frequency Carrier** as well as **Alternate Frequency Carrier 1** and **Alternate Frequency Carrier 2** on an AP's or BHMs Configuration => Radio page. Avoiding the TDWR band addresses FCC concerns about possible interference caused by Part 15 devices.

Operators with 5.4-GHz APs or BHMs set to a **Region Code** of **United States** are well-served to ensure they are not using any of the unavailable channels before upgrading. Operators may need to perform channel planning and coordinated change of the transmitting channel on APs or BHMs *before* the upgrade.

> *CAUTION!*
> ***Before*** upgrading a P10 or P11 5.4-GHz ***FSK*** AP or BHM with a **Region Code** of **United States** to Release 9.5, ensure that it is not configured with a center channel of **5590 through 5660 MHz**.
>
>
> ***Before*** upgrading a 5.4-GHz ***OFDM*** AP or BHM with a **Region Code** of **United States** to Release 9.5, ensure that it is not configured with a center channel of **5600 through 5650 MHz**.

If an affected AP or BHM is inadvertently left set to one of these center channels before upgrading, after the upgrade it will not have an operating **Radio Frequency Carrier** configured, will not transmit, and there will be no link or service to SMs or a BHS. To recover after the upgrade, configure the **Radio Frequency Carrier** of the AP or the BHM to an available channel – one displayed on the AP's or BHM's Configuration => Radio page.

Similarly, if the **Alternate Frequency Carrier 1** or **Alternate Frequency Carrier 2** is inadvertently left set to one of these center channels**,** the alternate frequencies will not be available in the case of a DFS event.

The **Custom Frequency Scan List** on SMs and BHSs set to a **Region Code** of **United States** is not affected. Since the center channel frequencies listed in Table 5 will not be used (the AP or BHM won't be transmitting on them) operators may want to disable scanning of these frequencies by the SMs and BHSs to reduce scan time.

Using Jitter to Check Received Signal Quality (FSK Only)

The General Status tab in the Home page of the SM and BHS displays current values for Jitter, which is essentially a measure of interference. Interpret the jitter value as indicated in Table 31.

Table 31: Signal quality levels indicated by jitter

Signal Modulation	Correlation of Highest Seen Jitter to Signal Quality		
	High Quality	Questionable Quality	Poor Quality
1X operation (2-level FSK)	0 to 4	5 to 14	15
2X operation (4-level FSK)	0 to 9	10 to 14	15

In your lab, an SM whose jitter value is constant at 14 may have an incoming packet efficiency of 100%. However, a deployed SM whose jitter value is 14 is likely to have even higher jitter values as interfering signals fluctuate in strength over time. So, *do not* consider 14 to be acceptable. Avoiding a jitter value of 15 should be the highest priority in establishing a link. At 15, jitter causes fragments to be dropped and link efficiency to suffer.

Modules calculate jitter based on both interference and the modulation scheme. For this reason, values on the low end of the jitter range that are significantly higher in 2X operation can still be indications of a high quality signal. For example, where the amount of interference remains constant, an SM with a jitter value of 3 in 1X operation can display a jitter value of 7 when enabled for 2X operation.

However, on the high end of the jitter range, *do not* consider the higher values in 2X operation to be acceptable. This is because 2X operation is much more susceptible to problems from interference than is 1X. For example, where the amount of interference remains constant, an SM with a jitter value of 6 in 1X operation can display a jitter value of 14 when enabled for 2X operation. As indicated in Table 31, these values are unacceptable.

OFDM uses a different modulation scheme and does not display a jitter value.

Using Link Efficiency to Check FSK Received Signal Quality

A link test, available in the Link Capacity Test tab of the Tools web page in an AP or BH, provides a more reliable indication of received signal quality, particularly if you launch tests of varying duration. However, a link test interrupts traffic and consumes system capacity, so *do not* routinely launch link tests across your networks.

Comparing Efficiency in 1X Operation to Efficiency in 2X Operation

Efficiency of at least 98 to 100% indicates a high quality signal. Check the signal quality numerous times, at various times of day and on various days of the week (as you checked the RF environment a variety of times by spectrum analysis before placing radios in the area). Efficiency less than 90% in 1X operation or less than 60% in 2X operation indicates a link with problems that require action.

When to Switch from 2X to 1X Operation Based on 60% Link Efficiency

In the above latter case (60% in 2X operation), the link experiences worse latency (from packet resends) than it would in 1X operation, but still greater capacity, if the link remains stable at 60% Efficiency. Downlink Efficiency and Uplink Efficiency are measurements produced by running a link test from either the SM or the AP. Examples of what action should be taken based on Efficiency in 2X operation are provided in Table 32.

Table 32: Recommended courses of action based on Efficiency in 2X operation

Module Types	Further Investigation	Result	Recommended Action
CAP 130 with CSM 130	Check the General Status tab of the CSM 130.[1] See Checking the Status of 2X Operation on Page 91.	Uplink and downlink are both ≥60% Efficiency.[2]	Rerun link tests.
	Rerun link tests.	Uplink and downlink are both ≥60% Efficiency.	Optionally, re-aim SM, add a reflector, or otherwise mitigate interference. In any case, continue 2X operation up and down.

Module Types	Further Investigation	Result	Recommended Action
CAP 130 with CSM 120	Check the General Status tab of the CSM 120.[1] See Checking the Status of 2X Operation on Page 91.	Uplink and downlink are both ≥60% Efficiency.[2]	Rerun link tests.
	Rerun link tests.	Uplink and downlink are both ≥60% Efficiency.	Optionally, re-aim SM, add a reflector, or otherwise mitigate interference. In any case, continue 2X operation up and down.
		Results are inconsistent and range from 20% to 80% Efficiency.	Monitor the Session Status tab in the CAP 130.
	Monitor the Session Status tab in the CAP 130.	Link fluctuates between 2X and 1X operation.[3]	Optionally, re-aim SM, add a reflector, or otherwise mitigate interference. Then rerun link tests.
	Rerun link tests.	No substantial improvement with consistency is seen.	On the General tab of the SM, disable 2X operation. Then rerun link tests.
	Rerun link tests.	Uplink and downlink are both ≥90% Efficiency.	Continue 1X operation up and down.

NOTES:

1. Or check Session Status page of the CAP 130, where a sum of greater than 7,000,000 bps for the up- and downlink indicates 2X operation up and down (for 2.4- or 5.x-GHz modules.
2. For throughput to the SM, this is equivalent to 120% Efficiency in 1X operation, with less capacity used at the AP.
3. This link is problematic.

Considering Frequency Band Alternatives

For 5.2-, 5.4-, and 5.7-GHz modules, 20-MHz wide channels are centered every 5 MHz. For 2.4-GHz modules, 20-MHz wide channels are centered every 2.5 MHz. For OFDM, the operator can configure center channel frequencies of the 10 MHz channels with a granularity of 0.5 MHz. This allows the operator to customize the channel layout for interoperability where other equipment is co-located.

Cross-band deployment of APs and BH is the recommended alternative (for example, a 5.2-GHz AP co-located with 5.7-GHz BH).

IMPORTANT!

In all cases, channel center separation between co-located FSK modules should be at least 20 MHz for 1X operation and 25 MHz for 2X. For OFDM, channel center separation between co-located modules should be at least 10 MHz.

900-MHz Channels

900-MHz AP Available Channels

A 900-MHz AP can operate with its 8-MHz wide channel centered on any of the following frequencies:

(All Frequencies in MHz)

906	909	912	915	918	922
907	910	913	916	919	923
908	911	914	917	920	924

900-MHz AP Cluster Recommended Channels

Three non-overlapping channels are recommended for use in a 900-MHz AP cluster:

(All Frequencies in MHz)

906	915	924

This recommendation allows 9 MHz of separation between channel centers. You can use the Spectrum Analysis feature in an SM, or use a standalone spectrum analyzer, to evaluate the RF environment. In any case, ensure that the 8-MHz wide channels you select *do not* overlap.

2.4-GHz Channels

2.4-GHz BHM and AP Available Channels

A 2.4-GHz BHM or AP can operate with its 20-MHz wide channel centered on any of the following channels, which are separated by only 2.5-MHz increments.

(All Frequencies in GHz)

2.4150	2.4275	2.4400	2.4525
2.4175	2.4300	2.4425	2.4550
2.4200	2.4325	2.4450	2.4575
2.4225	2.4350	2.4475	
2.4250	2.4375	2.4500	

The center channels of *adjacent* 2.4-GHz APs should be separated by at least 20 MHz.

2.4-GHz AP Cluster Recommended Channels

Three non-overlapping channels are recommended for use in a 2.4-GHz AP cluster:

(All Frequencies in GHz)

2.4150 2.4350 2.4575

This recommendation allows 20 MHz of separation between one pair of channels and 22.5 MHz between the other pair. You can use the Spectrum Analysis feature in an SM or BHS, or use a standalone spectrum analyzer, to evaluate the RF environment. Where spectrum analysis identifies risk of interference for any of these channels, you can compromise this recommendation as follows:

- Select 2.4375 GHz for the middle channel
- Select 2.455 GHz for the top channel
- Select 2.4175 GHz for the bottom channel

In any case, ensure that your plan allows at least 20 MHz of separation between channels.

4.9-GHz OFDM Channels

Channel selections for the OFDM AP in the 4.9-GHz frequency band range are 4.945 through 4.985 GHz on 5-MHz centers, with not more than five non-overlapping channels.

5.2-GHz Channels

Channel selections for the AP in the 5.2-GHz frequency band range depend on whether the AP is deployed in cluster.

5.2-GHz BH and Single AP Available Channels

A BH or a single 5.2-GHz AP can operate in the following channels, which are separated by 5-MHz increments.

(All Frequencies in GHz)

5.275	5.290	5.305	5.320
5.280	5.295	5.310	5.325
5.285	5.300	5.315	

The center channels of *adjacent* APs should be separated by at least 20 MHz. However, 25 MHz of separation is advised, especially for CAP 130s to take advantage of 2X operation.

5.2-GHz AP Cluster Recommended Channels

Three non-overlapping channels are recommended for use in a 5.2-GHz AP cluster:

(All Frequencies in GHz)

5.275	5.300	5.325

5.4-GHz FSK Channels

Channel selections for the AP in the 5.4-GHz FSK frequency band range depend on whether the AP is deployed in cluster.

5.4-GHz BH and Single AP Available

A BH or single 5.4-GHz FSK AP can operate in the following channels, which are separated by 5-MHz.

(All Frequencies in GHz)

5495	5515	5535	5555	5575	5595	5615	5635	5655	5675	5695
5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700
5505	5525	5545	5565	5585	5605	5625	5645	5665	5685	5705
5510	5530	5550	5570	5590	5610	5630	5650	5670	5690	

The channels of *adjacent* APs should be separated by at least 20 MHz, especially for CAP 130s to take advantage of 2X operation.

5.4-GHz AP Cluster Recommended Channels

The fully populated cluster requires only three channels, each reused by the module that is mounted 180° opposed. In this frequency band range, the possible sets of three non-overlapping channels are numerous. As many as 11 non-overlapping 20-MHz wide channels are available for 1X operation. Fewer 25-MHz wide channels are available for 2X operation, where this greater separation is recommended for interference avoidance.

5.4-GHz AP Cluster Limit Case

In the limit, the 11 channels could support all of the following, vertically stacked on the same mast:

- 3 full clusters, each cluster using 3 channels
- a set of 4 APs, the set using the 2 channels that no AP in any of the 3 full clusters is using

IMPORTANT!

Where regulations require you to have Dynamic Frequency Selection (DFS) enabled, analyze the spectrum, then spread your channel selections as evenly as possible throughout this frequency band range, appropriately sharing it with satellite services.

5.4-GHz OFDM Channels

Channel selections for the PMP 400 Series AP in the 5.4-GHz frequency band range depend on whether the AP is deployed.

5.4-GHz Single OFDM AP Available Channels

Operators configure the channels of OFDM modules on their Configuration => Custom Frequencies web pages. The available center channels for an individual OFDM AP (not in cluster) depends on the region where the AP is deployed and are in the ranges quoted in Table 33.

Table 33: Available center channels for single OFDM AP

Region	Range(s) For Center Channels[1]
U.S.A.	5480 to 5710
Canada	5480 to 5595 5655 to 5710
Europe	5475 to 5595 5655 to 5715
NOTES: 1. Selectable in 5-MHz increments.	

5.4-GHz OFDM AP Cluster Recommended Channels

No guard band is required between 10-MHz channels. However, to use the 3X operation feature of these OFDM modules, you should separate the channels of clustered APs by at least 10 MHz. The fully populated cluster may be configured for two channels—each reused by the module that is mounted 180° opposed—or four channels.

Channels are preconfigured to help in your decision on the two or four to use in a four-AP cluster. These modules *do not* include a spectrum analyzer for you to read the strength of neighboring frequencies. The ranges of available center channels for clustered APs are those shown in Table 33 above.

However, where 5.4-GHz OFDM APs are co-located with 5.4-GHz FSK APs, you should allow 25 MHz channel center spacing to prevent either of the sectors from experiencing interference from the other.

5.7-GHz Channels

Channel selections for the AP in the 5.7-GHz frequency band range depend on whether the AP is deployed in cluster.

5.7-GHz BH and Single AP Available Channels

A BH or a single 5.7-GHz AP enabled for frequencies can operate in the following channels, which are separated by 5-MHz increments.

(All Frequencies in GHz)

5.735	5.765	5.795	5.825
5.740	5.770	5.800	5.830
5.745	5.775	5.805	5.835
5.750	5.780	5.810	5.840
5.755	5.785	5.815	
5.760	5.790	5.820	

The channels of *adjacent* APs should be separated by at least 20 MHz. However, 25 MHz of separation is advised, especially for CAP 130s to take advantage of 2X operation.

5.7-GHz AP Cluster Recommended Channels

Six non-overlapping channels are recommended for use in 5.7-GHz AP clusters:

(All Frequencies in GHz)

5.735	5.775	5.815
5.755	5.795	5.835

The fully populated cluster requires only three channels, each reused by the module that is mounted 180° offset. The six channels above are also used for backhaul point-to-point links.

As noted above, a 5.7-GHz AP can operate on a frequency as high as 5.840 GHz. Where engineering plans allow, this frequency can be used to provide an additional 5-MHz separation between AP and BH channels.

Channels Available for PTP 400 and PTP 600 Radios

Channel selections for radios in the PTP400 and PTP 600 series are quoted in the user guides that are dedicated to those products. However, these units dynamically change channels when the signal substantially degrades. Since the available channels are in the 5.4- and 5.7-GHz frequency band ranges, carefully consider the potential effects of deploying these products into an environment where traffic in this range pre-exists.

Example Channel Plans for FSK AP Clusters

Examples for assignment of frequency channels and sector IDs are provided in the following tables. Each frequency is reused on the sector that is at a 180° offset. The entry in the Symbol column of each table refers to the layout in Figure 36 on Page 142.

NOTE:
The operator specifies the sector ID for the module as described under Sector ID on Page 541.

Table 34: Example 900-MHz channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	906 MHz	0	A
Northeast (60°)	915 MHz	1	B
Southeast (120°)	924 MHz	2	C
South (180°)	906 MHz	3	A
Southwest (240°)	915 MHz	4	B
Northwest (300°)	924 MHz	5	C

Table 35: Example 2.4-GHz channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	2.4150 GHz	0	A
Northeast (60°)	2.4350 GHz	1	B
Southeast (120°)	2.4575 GHz	2	C
South (180°)	2.4150 GHz	3	A
Southwest (240°)	2.4350 GHz	4	B
Northwest (300°)	2.4575 GHz	5	C

Table 36: Example 5.2-GHz channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	5.275 GHz	0	A
Northeast (60°)	5.300 GHz	1	B
Southeast (120°)	5.325 GHz	2	C
South (180°)	5.275 GHz	3	A
Southwest (240°)	5.300 GHz	4	B
Northwest (300°)	5.325 GHz	5	C

Table 37: Example 5.4-GHz channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	5.580 GHz	0	A
Northeast (60°)	5.620 GHz	1	B
Southeast (120°)	5.660 GHz	2	C
South (180°)	5.580 GHz	3	A
Southwest (240°)	5.620 GHz	4	B
Northwest (300°)	5.660 GHz	5	C

Table 38: Example 5.7-GHz FSK channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	5.735 GHz	0	A
Northeast (60°)	5.755 GHz	1	B
Southeast (120°)	5.775 GHz	2	C
South (180°)	5.735 GHz	3	A
Southwest (240°)	5.755 GHz	4	B
Northwest (300°)	5.775 GHz	5	C

Multiple FSK Access Point Clusters

When deploying multiple AP clusters in a dense area, consider aligning the clusters as shown in Figure 36. However, this is only a recommendation. An installation may dictate a different pattern of channel assignments.

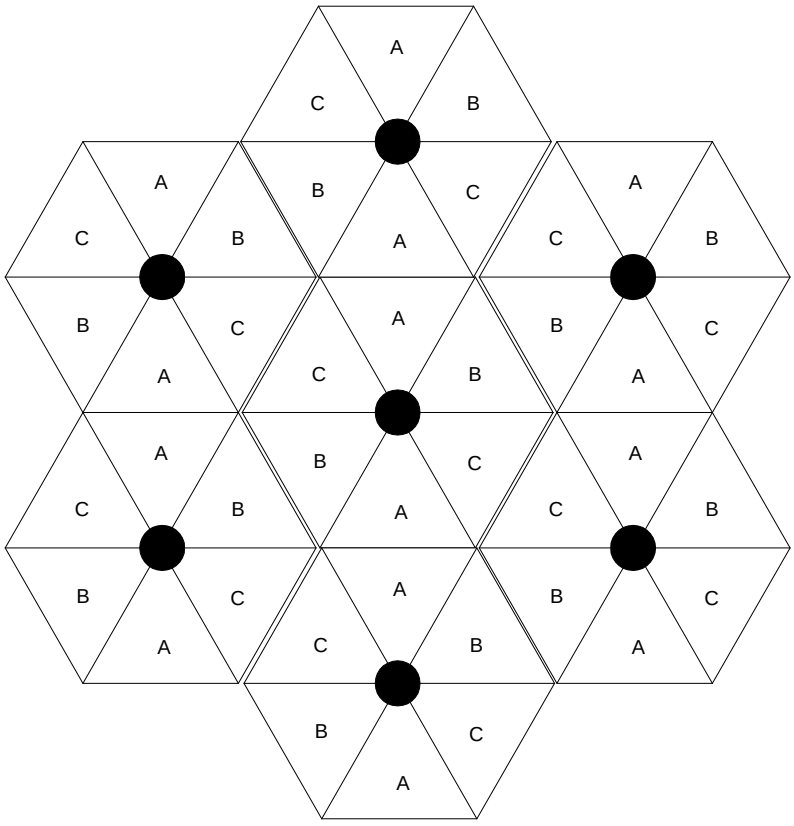
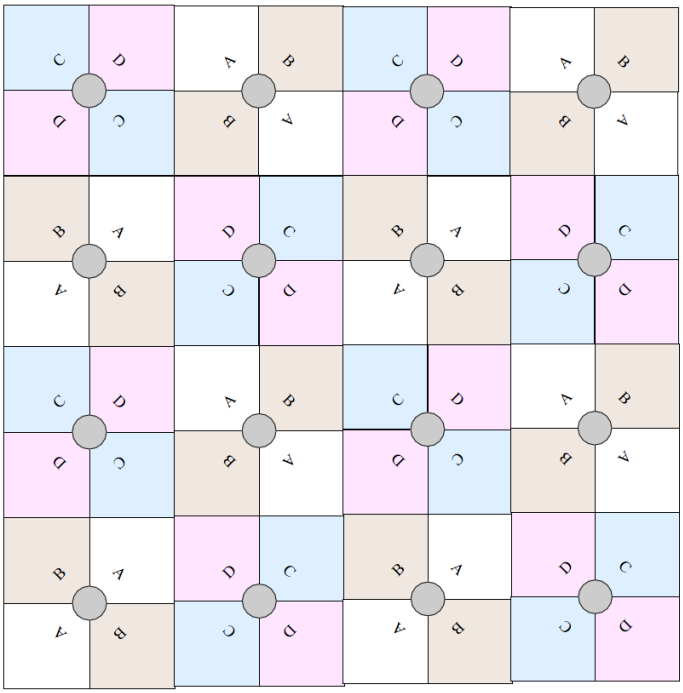


Figure 36: Example layout of 7 FSK Access Point clusters

Multiple OFDM Access Point Clusters

When deploying multiple AP clusters in a dense area, consider aligning the clusters as shown below. However, this is only a recommendation. An installation may dictate a different pattern of channel assignments.

Figure 37: Example layout of 16 Access Point sectors (ABCD), 90 degree sectors

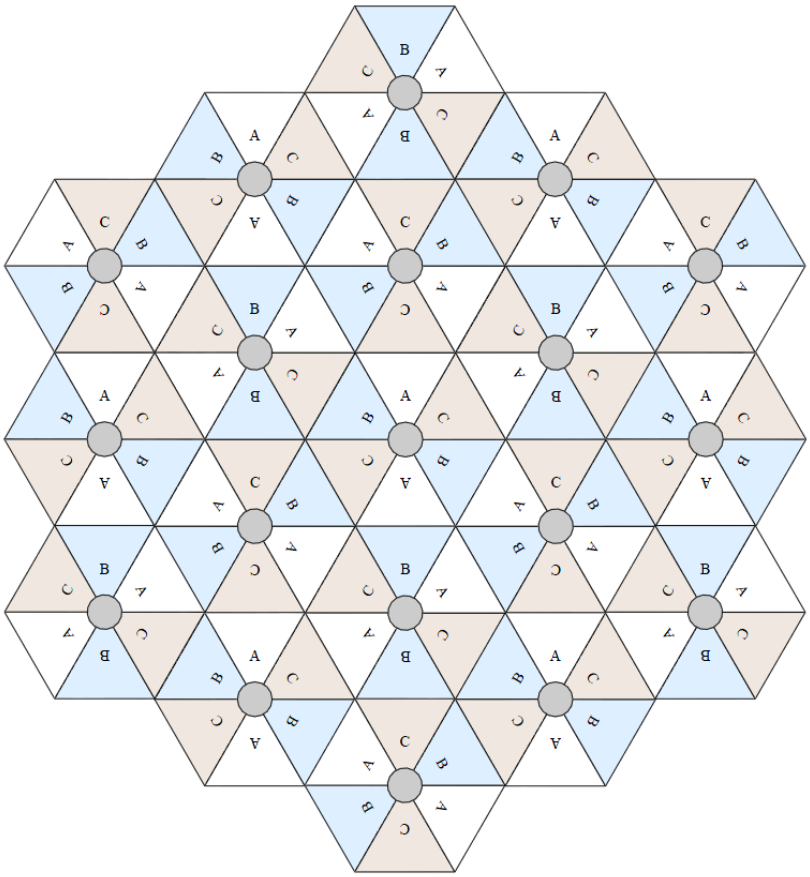


An example for assignment of frequency channels and sector IDs is provided in the following table.

Table 39: Example 5.8-GHz OFDM channel assignment by sector, 5 MHz guard band between adjacent sectors

Symbol	Frequency	Sector ID
A	5.735 GHz	0
B	5.760 GHz	1
C	5.785 GHz	2
D	5.810 GHz	3

Figure 38: Example layout of 16 Access Point sectors (ABC), 60 degree sectors



An example for assignment of frequency channels and sector IDs is provided in the following table.

Table 40: Example 5.8-GHz OFDM channel assignment by sector, 5 MHz guard band between adjacent sectors

Symbol	Frequency	Sector ID
A	5.735 GHz	0
B	5.760 GHz	1
C	5.785 GHz	2

Selecting Sites for Network Elements

The APs must be positioned

- with hardware that the wind and ambient vibrations cannot flex or move.

- where a tower or rooftop is available or can be erected.
- where a grounding system is available.
- with lightning arrestors to transport lightning strikes away from equipment.
- at a proper height:
  - higher than the tallest points of objects immediately around them (such as trees, buildings, and tower legs).
  - at least 2 feet (0.6 meters) below the tallest point on the tower, pole, or roof (for lightning protection).
- away from high-RF energy sites (such as AM or FM stations, high-powered antennas, and live AM radio towers).
- in line-of-sight paths
  - to the SMs and BH.
  - that will not be obstructed by trees as they grow or structures that are later built.

NOTE:
Visual line of sight does not guarantee radio line of sight.

Surveying Sites

Factors to survey at potential sites include

- what pre-existing wireless equipment exists at the site. (Perform spectrum analysis.)
- whether available mounting positions exist near the lowest elevation that satisfies line of site, coverage, and other link criteria.
- whether you will always have the right to decide who climbs the tower to install and maintain your equipment, and whether that person or company can climb at any hour of any day.
- whether you will have collaborative rights and veto power to prevent interference to your equipment from wireless equipment that is installed at the site in the future.
- whether a pre-existing grounding system (path to Protective Earth ⏚) exists, and what is required to establish a path to it.
- who is permitted to run any indoor lengths of cable.

Assuring the Essentials

In the 2.4-, 5.2-, 5.4-, and 5.7-GHz frequency band ranges, an unobstructed line of sight (LOS) must exist and be maintainable between the radios that are involved in each link.

Line of Sight (LOS) Link

In these ranges, a line of sight link is both

- an unobstructed straight line from radio to radio.
- an unobstructed zone surrounding that straight line.

Fresnel Zone Clearance

An unobstructed line of sight is important, but is not the *only* determinant of adequate placement. Even where the path has a clear line of sight, obstructions such as terrain, vegetation, metal roofs, or cars may penetrate the Fresnel zone and cause signal loss. Figure 39 illustrates an ideal Fresnel zone.

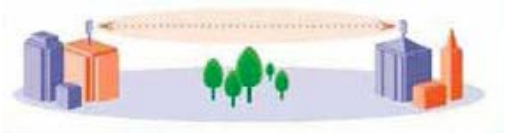


Figure 39: Fresnel zone in line of sight link

Near Line of Sight (nLOS) Link

The 900-MHz and OFDM modules have a greater near line of sight (nLOS) range than modules of other frequency bands. NLOS range depends on RF considerations such as foliage, topography, obstructions. A depiction of an nLOS link is shown in Figure 40.

Figure 40: Fresnel zone in near line of sight link

Non-Line of Sight (NLOS) Link

The 900-MHz and OFDM modules have a greater non-line of sight (NLOS) range than modules of other frequency bands. NLOS range depends on RF considerations such as foliage, topography, obstructions. A depiction of an NLOS link is shown in Figure 41.

Figure 41: Fresnel zone in non-line of sight link

Clearing the Radio Horizon

Because the surface of the earth is curved, higher module elevations are required for greater link distances. This effect can be critical to link connectivity in link spans that are greater than 8 miles (12 km).

To use metric units to find the minimum height required to reach the radio horizon use the following equation:

Radio horizon distance (km) = 4.12 (SQRT(h1) + SQRT(h2))

Where:	Is:
h1	height of the AP
h2	height of the SM

To use English standard units to find the angle of elevation, use the following formula:

Radio horizon distance (km) = 1.42 (SQRT(h1) + SQRT(h2))

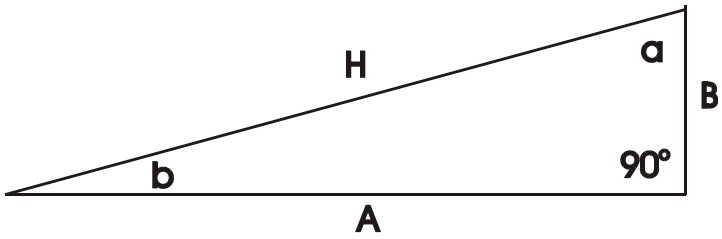
Where:	Is:
h1	height of the AP
h2	height of the SM

Calculating the Aim Angles

The proper angle of tilt can be calculated as a factor of both the difference in elevation and the distance that the link spans. Even in this case, a plumb line and a protractor can be helpful to ensure the proper tilt. This tilt is typically minimal.

The number of degrees to offset (from vertical) the mounting hardware leg of the support tube is equal to the angle of elevation from the lower module to the higher module (<B in the example provided in Figure 42).

Figure 42: Variables for calculating angle of elevation (and depression)



Where:	Is:
b	angle of elevation
B	vertical difference in elevation
A	horizontal distance between modules

Calculating the Angle of Elevation

To use metric units to find the angle of elevation, use the following formula:

$$\tan b = \frac{B}{1000A}$$

Where:	Is:
B	expressed in meters
A	expressed in kilometers

To use English standard units to find the angle of elevation, use the following formula:

$$\tan b = \frac{B}{5280A}$$

Where:	Is:
B	expressed in feet
A	expressed in miles

The angle of depression from the higher module is identical to the angle of elevation from the lower module.

Co-locating Modules

A BH and an AP or AP cluster on the same tower require a CMM. The CMM properly synchronizes the *transmit start* times of all modules to prevent interference and desensing of the modules. At closer distances without sync from a CMM, the frame structures cause self interference.

Furthermore, a BH and an AP on the same tower require that the effects of their differing *receive start* times be mitigated by either

- 100 vertical feet (30 meters) or more and as much spectral separation as possible within the same frequency band range.
- the use of the frame calculator to tune the **Downlink Data** parameter in each, so that the receive start time in each is the same. See Using the Frame Calculator Tool (All) on Page 542.

APs and a BHS can be co-located at the same site only if they operate in different frequency band ranges.

Where a single BH air link is insufficient to cover the distance from an AP cluster to your point of presence (POP), you can deploy two BHSs, connected to one another by Ethernet, on a tower that is between a BHM co-located with the AP cluster and another BHM co-located with the POP. This deployment is illustrated in Figure 43.

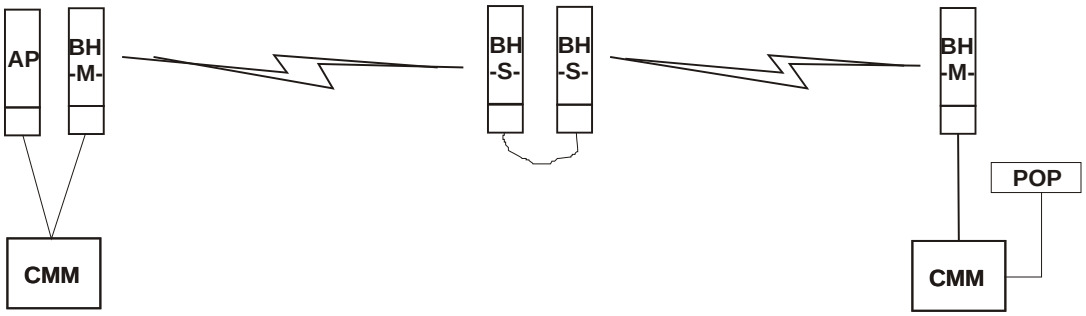


Figure 43: Double-hop backhaul links

However, the BHSs can be co-located at the same site *only if* one is on a different frequency band range from that of the other or one of the following conditions applies:

- They are vertically separated on a structure by at least 100 feet (30 m).
- They are vertically separated on a structure by less distance, but either
  - an RF shield isolates them from each other.
  - the uplink and downlink data parameters and control channels match (the **Downlink Data** parameter is set to **50%**).

The constraints for co-located modules in the same frequency band range are to avoid self-interference that would occur between them. Specifically, unless the uplink and downlink data percentages match, intervals exist when one is transmitting while the other is receiving, such that the receiving module cannot receive the signal from the far end.

The interference is less a problem during low throughput periods and intolerable during high. Typically, during low throughput periods, sufficient time exists for the far end to retransmit packets lost because of interference from the co-located module.

Deploying a Remote AP

In cases where the subscriber population is widely distributed, or conditions such as geography restrict network deployment, you can add a Remote AP to

- provide high-throughput service to near LoS business subscribers.
- reach around obstructions or penetrate foliage with non-LoS throughput.
- reach new, especially widely distributed, residential subscribers with broadband service.
- pass sync to an additional RF hop.

In the remote AP configuration, a remote AP is co-located with an SM. The remote AP distributes the signal over the last mile to SMs that are logically behind the co-located SM. A remote AP deployment is illustrated in Figure 44.

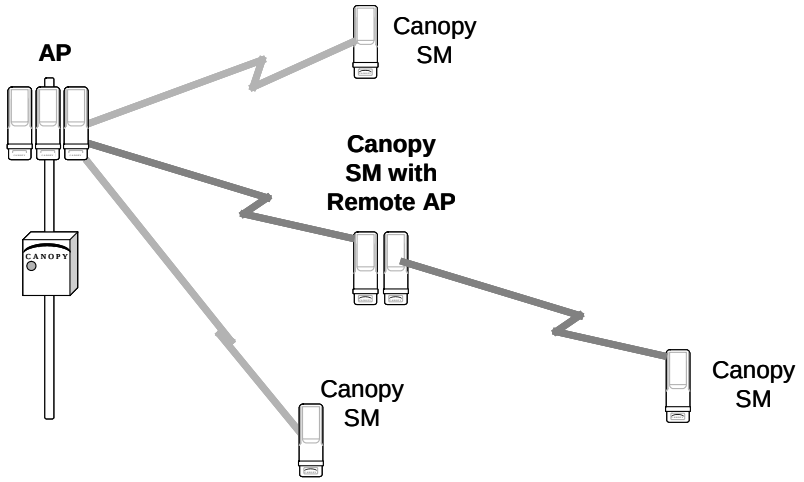


Figure 44: Remote AP deployment

The co-located SM receives data in one frequency band, and the remote AP must redistribute the data in a different frequency band. Base your selection of frequency band ranges on regulatory restrictions, environmental conditions, and throughput requirements.

IMPORTANT!
Each relay hop (additional daisy-chained remote AP) adds approximately 6 msec latency.

Remote AP Performance

The performance of a remote AP is identical to the AP performance in cluster. Throughputs, ranges, and patch antenna coverage are identical. CAP 130s and CSM 130s (or CAP 09130s and CSM 09130s) can be deployed in tandem in the same sector to meet customer bandwidth demands.

As with all equipment operating in the unlicensed spectrum, Cambium *strongly* recommends that you perform site surveys before you add network elements. These will indicate that spectrum is available in the area where you want to grow. Keep in mind that

- non-LoS ranges heavily depend on environmental conditions.
- in most regions, not all frequencies are available.
- your deployments must be consistent with local regulatory restrictions.

Example Use Case for RF Obstructions

A remote AP can be used to provide last-mile access to a community where RF obstructions prevent SMs from communicating with the higher-level AP in cluster. For example, you may be able to use 900 MHz for the last mile between a remote AP and the outlying SMs where these subscribers cannot form good links to a higher-level 2.4-GHz AP. In this case, the short range of the 900-MHz remote AP is sufficient, and the ability of the 900-MHz wavelength to be effective around foliage at short range solves the foliage penetration problem.

An example of this use case is shown in Figure 45.

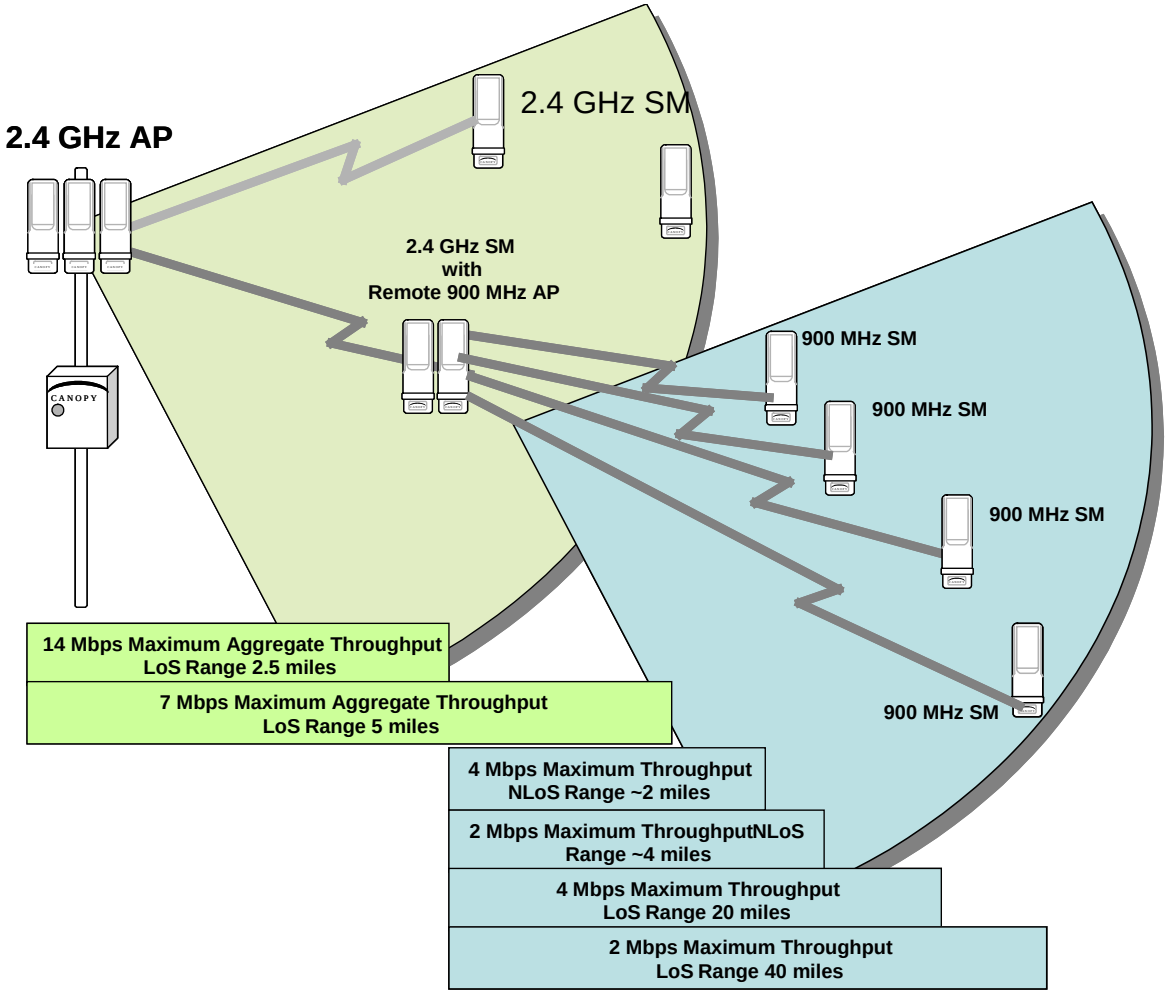


Figure 45: Example 900-MHz remote AP behind 2.4-GHz SM

The 2.4 GHz modules provide a sustained aggregate throughput of up to 14 Mbps to the sector. One of the SMs in the sector is wired to a 900-MHz remote AP, which provides NLoS sustained aggregate throughput[4] of

[4] NLoS ranges depend on environmental conditions. Your results may vary from these.

- 4 Mbps to 900-MHz SMs up to 2 miles away in the sector.
- 2 Mbps to 900-MHz SMs between 2 and 4 miles away in the sector.

Example Use Case for Passing Sync

All radios support the remote AP functionality. The BHS and the SM can reliably pass the sync pulse, and the BHM and AP can reliably receive it. Examples of passing sync over cable are shown under Passing Sync in an Additional Hop on Page 96. The sync cable is described under Cables on Page 57.

The sync is passed in a cable that connects Pins 1 and 6 of the RJ-11 timing ports of the two modules. When you connect modules in this way, you must also adjust configuration parameters to ensure that

- the AP is set to properly receive sync.
- the SM will not propagate sync to the AP if the SM itself ceases to receive sync.

Perform Procedure 33: Extending network sync on Page 426.

Physical Connections Involving the Remote AP

The SM to which you wire a remote AP can be either an SM that serves a customer or an SM that simply serves as a relay. Where the SM serves a customer, wire the remote AP to the SM as shown in Figure 46.

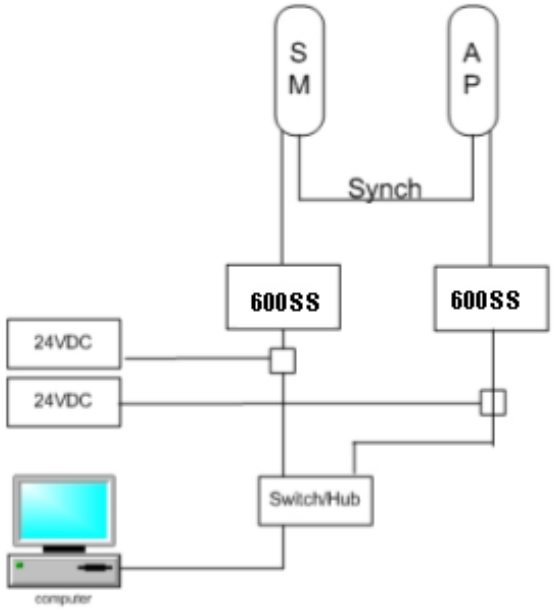


Figure 46: Remote AP wired to SM that also serves a customer

Where the SM simply serves as a relay, you must use a straight-through RJ-45 female-to-female coupler, and wire the SM to the remote AP as shown in Figure 47.

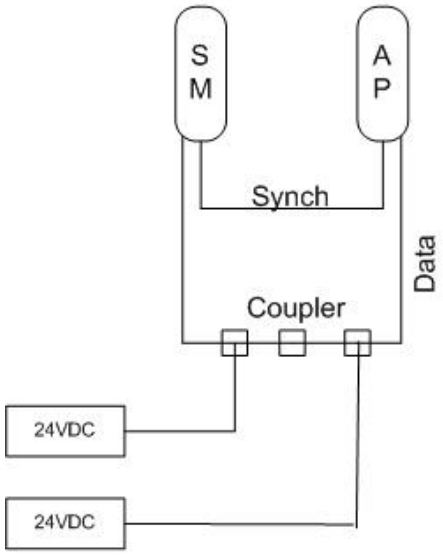


Figure 47: Remote AP wired to SM that serves as a relay

Diagramming Network Layouts

Accounting for Link Ranges and Data Handling Requirements

For aggregate throughput correlation to link distance in both point-to-multipoint and point-to-point links, see

- Link Performance and Encryption Comparisons on Page 62.
- all regulations that apply in your region and nation(s).

Avoiding Self Interference

For 5.2-, 5.4-, and 5.7-GHz modules, 20-MHz wide channels are centered every 5 MHz. For 2.4-GHz modules, 20-MHz wide channels are centered every 2.5 MHz. For 5.4-GHz OFDM modules, 10-MHz wide channels can be centered every 0.5 MHz. This allows you to customize the channel layout for interoperability where other equipment is co-located, as well as select channels with the least background interference level.

CAUTION!
Regardless of whether 2.4-, 5.2-, 5.4-, or 5.7-GHz modules are deployed, channel separation between modules should be at least 20 MHz for 1X operation or 25 MHz for 2X.

Physical Proximity

A BH and an AP on the same tower require a CMM. The CMM properly synchronizes the *transmit start* times of all modules to prevent interference and desensing of the modules. At closer distances without sync from a CMM, the frame structures cause self interference.

Furthermore, a BH and an AP on the same tower require that the effects of their differing *receive start* times be mitigated by either

- 100 vertical feet (30 meters) or more and as much spectral separation as possible within the same frequency band range.
- the use of the frame calculator to tune the Downlink Data % parameter in each, so that the receive start time in each is the same. See Using the Frame Calculator Tool (All) on Page 542.

Spectrum Analysis

You can use an SM or BHS as a spectrum analyzer. See Mapping RF Neighbor Frequencies on Page 125. Through a toggle of the **Device Type** parameter, you can temporarily transform an AP into an SM to use it as a spectrum analyzer.

Power Reduction to Mitigate Interference

Where any module (SM, AP, BH timing master, or BH timing slave) is close enough to another module that self-interference is possible, you can set the SM to operate at less than full power. To do so, perform the following steps.

CAUTION!
Too low a setting of the **Transmitter Output Power** parameter can cause a link to a distant module to drop. A link that drops for this reason requires Ethernet access to the GUI to re-establish the link.

Procedure 3: Reducing transmitter output power

1. Access the Radio tab of the module.
2. In the **Transmitter Output Power** parameter, reduce the setting.
3. Click **Save Changes**.
4. Click **Reboot**.
5. Access the Session Status tab in the Home web page of the SM.

6. Assess whether the link achieves good **Power Level** and **Jitter** values.
   NOTE: The received **Power Level** is shown in dBm and should be maximized. **Jitter**, where a value is present, should be minimized. However, better/lower jitter should be favored over better/higher dBm. For historical reasons, **RSSI** is also shown and is the unitless measure of power. The best practice is to use **Power Level** and ignore **RSSI**, which implies more accuracy and precision than is inherent in its measurement.
7. Access the Link Capacity Test tab in the Tools web page of the module.
8. Assess whether the desired links for this module achieve
   - uplink efficiency greater than 90%.
   - downlink efficiency greater than 90%.
9. If the desired links fail to achieve any of the above measurement thresholds, then
   a. access the module by direct Ethernet connection.
   b. access the Radio tab in the Configuration web page of the module.
10. In the **Transmitter Output Power** parameter, increase the setting.
11. Click **Save Changes**.
12. Click **Reboot**.

Avoiding Other Interference

Where signal strength cannot dominate noise levels, the network experiences

- bit error corrections.
- packet errors and retransmissions.
- lower throughput (because bandwidth is consumed by retransmissions) and high latency (due to resends).

Be especially cognitive of these symptoms for 900-MHz links. Where you see these symptoms, attempt the following remedies:

- Adjust the position of the SM.
- Deploy a band-pass filter at the AP.
- Consider adding a remote AP closer to the affected SMs. (See Deploying a Remote AP on Page 150.)

Certain other actions, which may seem to be potential remedies, *do not* resolve high noise level problems:

- *Do not* deploy an omnidirectional antenna.
- *Do not* set the antenna gain above the regulated level.
- *Do not* deploy a band-pass filter in the expectation that this can mitigate co-channel interference.

Chapter 13: Engineering Your IP Communications

Understanding Addresses

A basic understanding of Internet Protocol (IP) address and subnet mask concepts is required for engineering your IP network.

IP Address

The IP address is a 32-bit binary number that has four parts (octets). This set of four octets has two segments, depending on the class of IP address. The first segment identifies the network. The second identifies the hosts or devices on the network. The subnet mask marks a boundary between these two sub-addresses.

Dynamic or Static Addressing

For any computer to communicate with a module, the computer must be configured to either

- use DHCP (Dynamic Host Configuration Protocol). In this case, when not connected to the network, the computer derives an IP address on the 169.254 network within two minutes.
- have an assigned static IP address (for example, 169.254.1.5) on the 169.254 network.

IMPORTANT!
If an IP address that is set in the module is not the 169.254.x.x network address, then the network operator must assign the computer a static IP address in the same subnet.

When a DHCP Server is Not Found

To operate on a network, a computer requires an IP address, a subnet mask, and possibly a gateway address. Either a DHCP server automatically assigns this configuration information to a computer on a network or an operator must input these items.

When a computer is brought on line and a DHCP server is not accessible (such as when the server is down or the computer is not plugged into the network), Microsoft and Apple operating systems default to an IP address of 169.254.x.x and a subnet mask of 255.255.0.0 (169.254/16, where /16 indicates that the first 16 bits of the address range are identical among all members of the subnet).

Network Address Translation (NAT)

NAT, DHCP Server, DHCP Client, and DMZ in SM

The system provides NAT (network address translation) for SMs in the following combinations of NAT and DHCP (Dynamic Host Configuration Protocol):

- NAT Disabled (as in earlier releases)
- NAT with DHCP Client (**DHCP** selected as the **Connection Type** of the WAN interface) and DHCP Server
- NAT with DHCP Client(**DHCP** selected as the **Connection Type** of the WAN interface)
- NAT with DHCP Server
- NAT without DHCP

NAT

NAT isolates devices connected to the Ethernet/wired side of an SM from being seen directly from the wireless side of the SM. With NAT enabled, the SM has an IP address for transport traffic (separate from its address for management), terminates transport traffic, and allows you to assign a range of IP addresses to devices that are connected to the Ethernet/wired side of the SM.

In the Cambium system, NAT supports many protocols, including HTTP, ICMP (Internet Control Message Protocols), and FTP (File Transfer Protocol). For virtual private network (VPN) implementation, L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) and PPTP (Point to Point Tunneling Protocol) are supported. See NAT and VPNs on Page 163.

DHCP

DHCP enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the Cambium system.

In conjunction with the NAT features, each SM provides

- a DHCP server that assigns IP addresses to computers connected to the SM by Ethernet protocol.
- a DHCP client that receives an IP address for the SM from a network DHCP server.

DMZ

In conjunction with the NAT features, a DMZ (demilitarized zone) allows the assignment of one IP address behind the SM for a device to logically exist outside the firewall and receive network traffic. The first three octets of this IP address must be identical to the first three octets of the NAT private IP address.

NAT Disabled

The NAT Disabled implementation is illustrated in Figure 48.

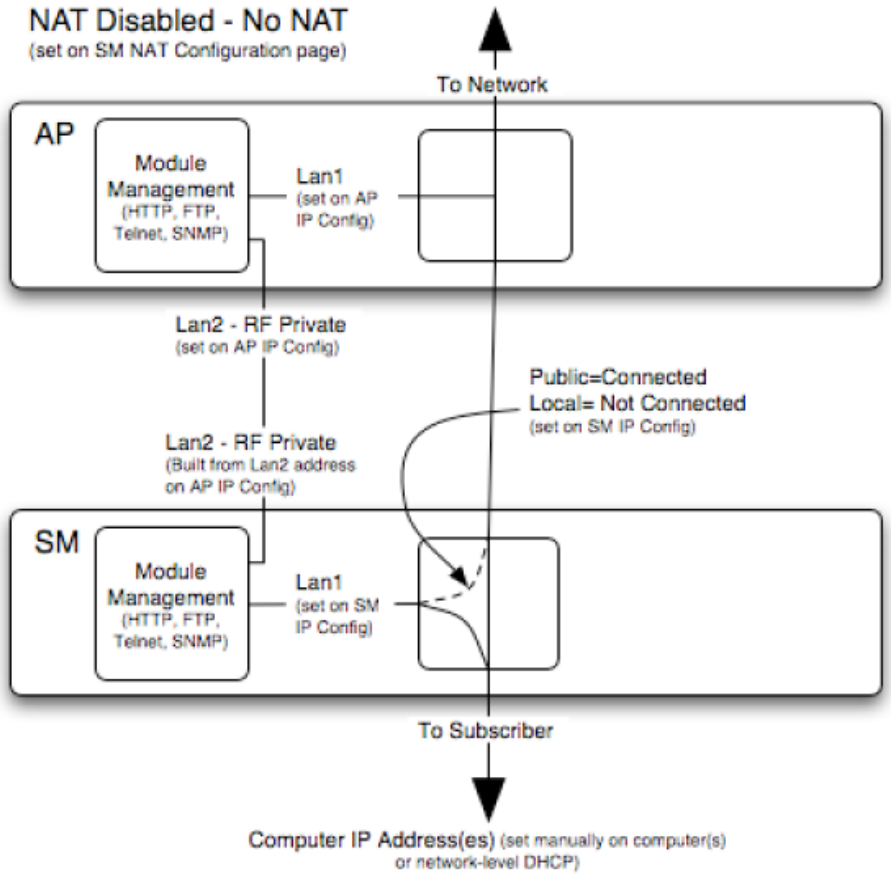

NAT Disabled - No NAT
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1 (set on AP IP Config)
Lan2 - RF Private (set on AP IP Config)
Public=Connected
Local= Not Connected
(set on SM IP Config)
Lan2 - RF Private (Built from Lan2 address on AP IP Config)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1 (set on SM IP Config)
To Subscriber
Computer IP Address(es) (set manually on computer(s) or network-level DHCP)

Figure 48: NAT Disabled implementation

NAT with DHCP Client and DHCP Server

The NAT with DHCP Client (**DHCP** selected as the **Connection Type** of the WAN interface) and DHCP Server implementation is illustrated in Figure 49.

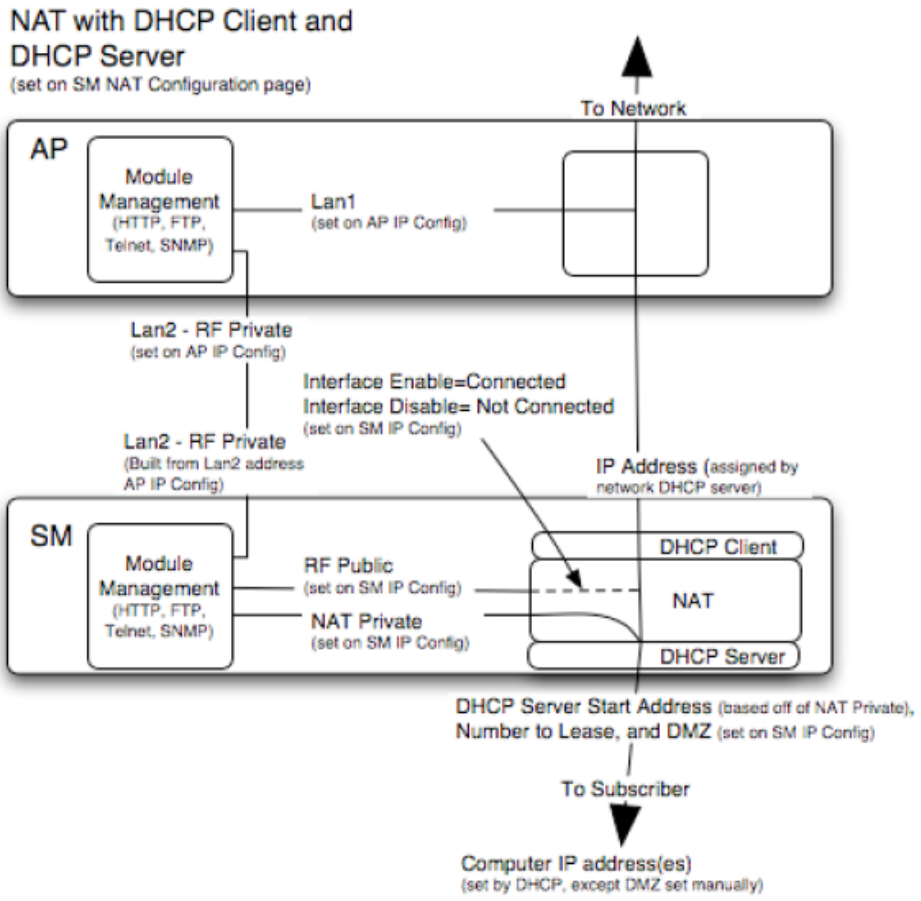

NAT with DHCP Client and DHCP Server
(set on SM NAT Configuration page)
To Network
AP
Module Management
(HTTP, FTP, Telnet, SNMP)
Lan1
(set on AP IP Config)
Lan2 - RF Private
(set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private
(Built from Lan2 address AP IP Config)
IP Address (assigned by network DHCP server)
SM
Module Management
(HTTP, FTP, Telnet, SNMP)
RF Public
(set on SM IP Config)
NAT Private
(set on SM IP Config)
DHCP Client
NAT
DHCP Server
DHCP Server Start Address (based off of NAT Private), Number to Lease, and DMZ (set on SM IP Config)
To Subscriber
Computer IP address(es)
(set by DHCP, except DMZ set manually)

Figure 49: NAT with DHCP Client and DHCP Server implementation

NAT with DHCP Client

The NAT with DHCP Client (**DHCP** selected as the **Connection Type** of the WAN interface) implementation is illustrated in Figure 50.

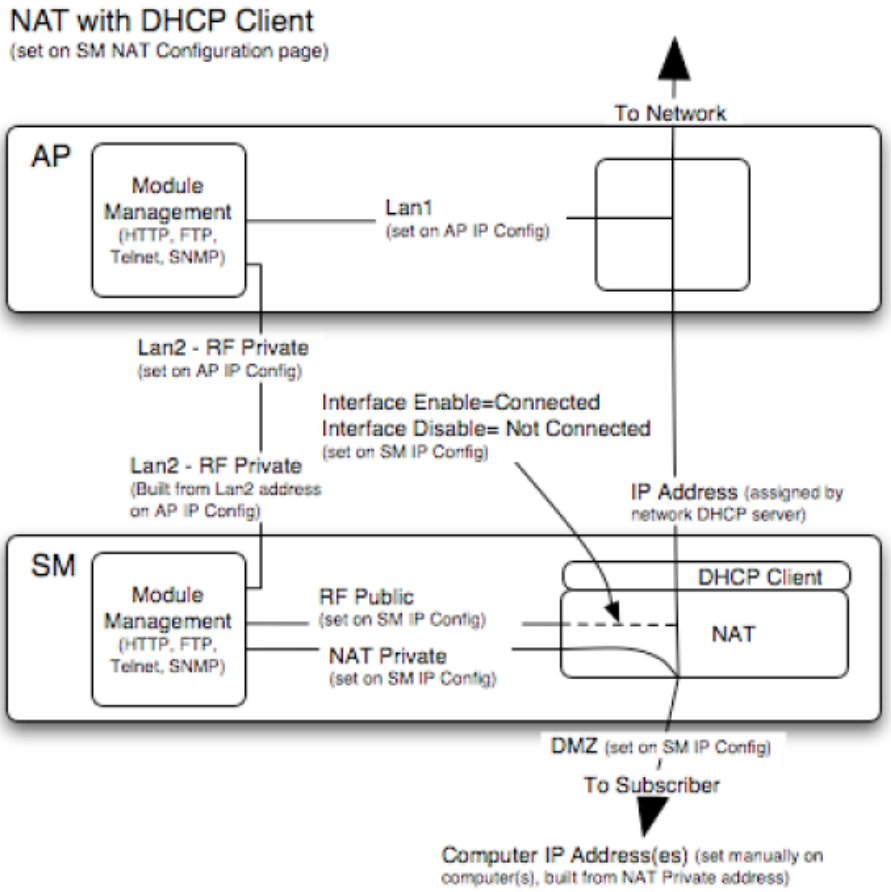

NAT with DHCP Client
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1
(set on AP IP Config)
Lan2 - RF Private
(set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private
(Built from Lan2 address on AP IP Config)
IP Address (assigned by network DHCP server)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
RF Public
(set on SM IP Config)
NAT Private
(set on SM IP Config)
DHCP Client
NAT
DMZ (set on SM IP Config)
To Subscriber
Computer IP Address(es) (set manually on computer(s), built from NAT Private address)

Figure 50: NAT with DHCP Client implementation

NAT with DHCP Server

The NAT with DHCP Server implementation is illustrated in Figure 51.

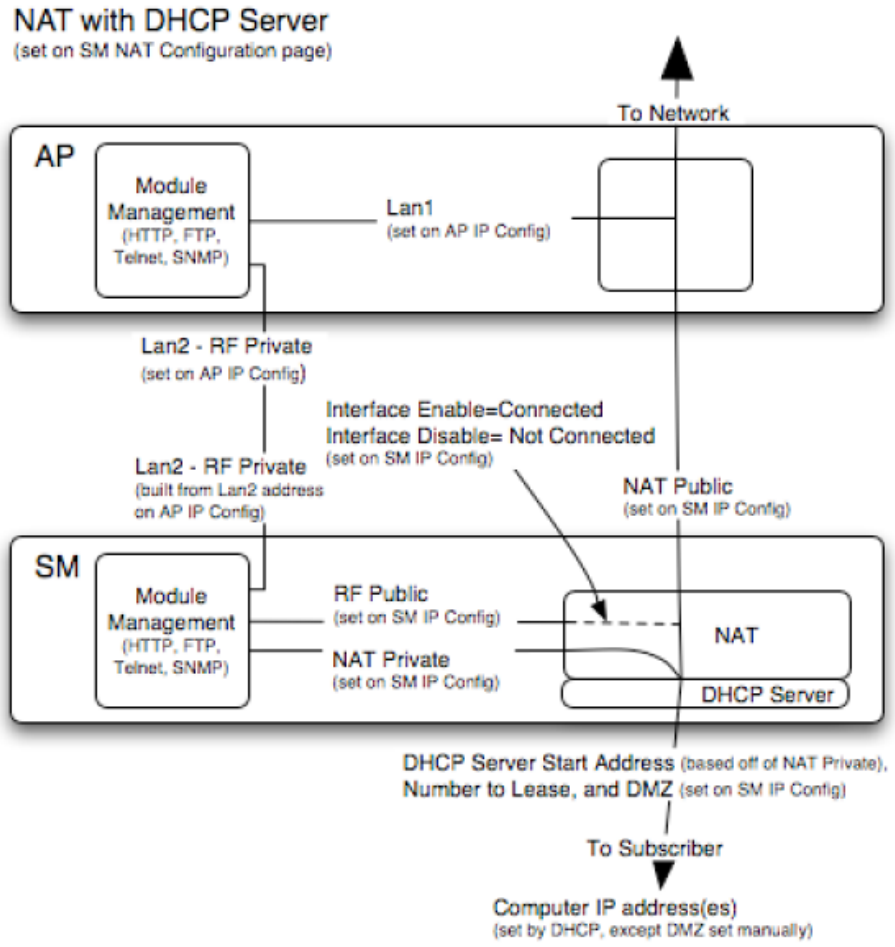

NAT with DHCP Server
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1
(set on AP IP Config)
Lan2 - RF Private
(set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private
(built from Lan2 address on AP IP Config)
NAT Public
(set on SM IP Config)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
RF Public
(set on SM IP Config)
NAT Private
(set on SM IP Config)
NAT
DHCP Server
DHCP Server Start Address (based off of NAT Private), Number to Lease, and DMZ (set on SM IP Config)
To Subscriber
Computer IP address(es)
(set by DHCP, except DMZ set manually)

Figure 51: NAT with DHCP Server implementation

NAT without DHCP

The NAT without DHCP implementation is illustrated in Figure 52.

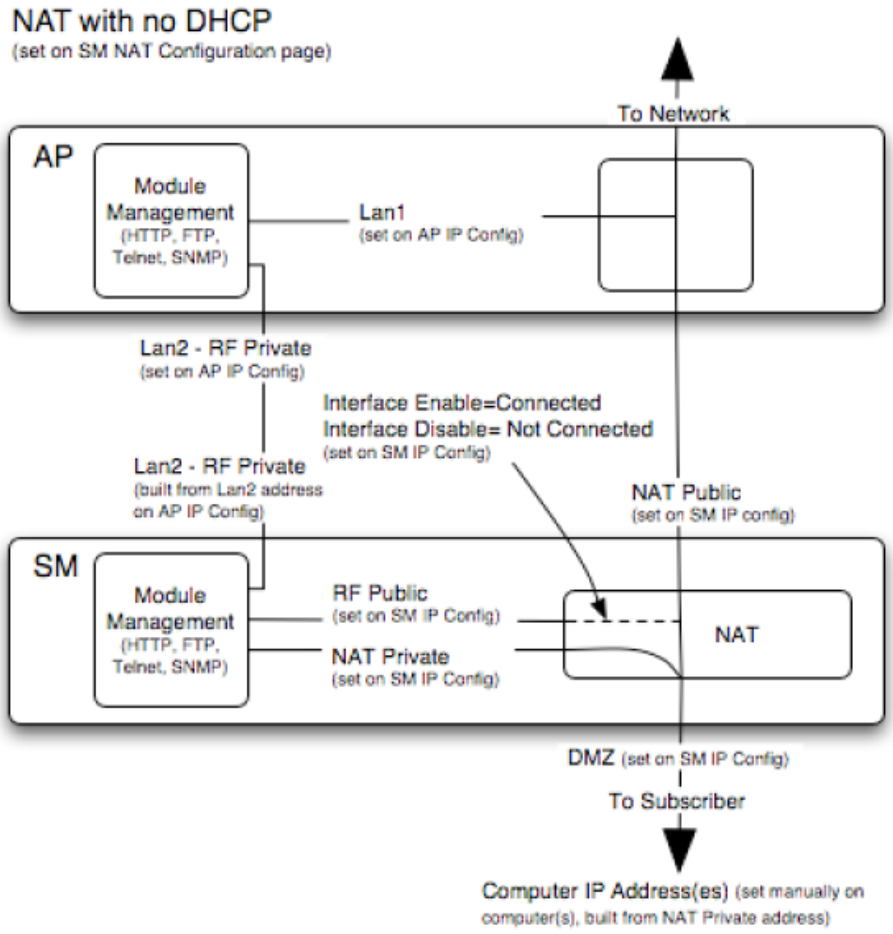


Figure 52: NAT without DHCP implementation

NAT and VPNs

VPN technology provides the benefits of a private network during communication over a public network. One typical use of a VPN is to connect remote employees, who are at home or in a different city, to their corporate network over the public Internet. Any of several VPN implementation schemes is possible. By design, NAT translates or changes addresses, and thus interferes with a VPN that is not specifically supported by a given NAT implementation.

With NAT enabled, SMs support L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) VPNs and PPTP (Point to Point Tunneling Protocol) VPNs. With NAT disabled, SMs support all types of VPNs.

Developing an IP Addressing Scheme

Network elements are accessed through IP Version 4 (IPv4) addressing.
A proper IP addressing method is critical to the operation and security of a network.

Each module requires an IP address on the network. This IP address is for only management purposes. For security, you should either

- assign an unroutable IP address.
- assign a routable IP address only if a firewall is present to protect the module.

You will assign IP addresses to computers and network components by either *static* or *dynamic* IP addressing. You will also assign the appropriate subnet mask and network gateway to each module.

Address Resolution Protocol

As previously stated, the MAC address identifies a module in

- communications between modules.
- the data that modules store about each other.
- the data that BAM or Prizm applies to manage authentication and bandwidth.

The IP address is essential for data delivery through a router interface. Address Resolution Protocol (ARP) correlates MAC addresses to IP addresses.

For communications to outside the network segment, ARP reads the network gateway address of the router and translates it into the MAC address of the router. Then the communication is sent to MAC address (physical network interface card) of the router.

For each router between the sending module and the destination, this sequence applies. The ARP correlation is stored until the ARP cache times out.

Allocating Subnets

The subnet mask is a 32-bit binary number that filters the IP address. Where a subnet mask contains a bit set to 1, the corresponding bit in the IP address is part of the network address.

Example IP Address and Subnet Mask

In Figure 53, the first 16 bits of the 32-bit IP address identify the network:

	Octet 1	Octet 2	Octet 3	Octet 4
IP address 169.254.1.1	10101001	11111110	00000001	00000001
Subnet mask 255.255.0.0	11111111	11111111	00000000	00000000

Figure 53: Example of IP address in Class B subnet

In this example, the network address is 169.254, and 2^{16} (65,536) hosts are addressable.

Selecting Non-routable IP Addresses

The factory default assignments for network elements are

- unique MAC address
- IP address of 169.254.1.1, except for an OFDM series BHM, whose IP address is 169.254.1.2 by default
- subnet mask of 255.255.0.0
- network gateway address of 169.254.0.0

For each radio and CMMmicro and CMM4, assign an IP address that is both consistent with the IP addressing plan for your network and cannot be accessed from the Internet. IP addresses within the following ranges are not routable from the Internet, regardless of whether a firewall is configured:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

You can also assign a subnet mask and network gateway for each CMMmicro and CMM4.

Translation Bridging

Optionally, you can configure the AP to change the source MAC address in every packet it receives from its SMs to the MAC address of the SM that bridged the packet, before forwarding the packet toward the public network. If you do, then

- not more than 10 IP devices at any time are valid to send data to the AP from behind the SM.
- the AP populates the Translation Table tab of its Statistics web page, displaying the MAC address and IP address of all the valid connected devices.
- each entry in the Translation Table is associated with the number of minutes that have elapsed since the last packet transfer between the connected device and the SM.
- if 10 are connected, and another attempts to connect

  - and no Translation Table entry is older than 255 minutes, the attempt is ignored.
  - and an entry is older than 255 minutes, the oldest entry is removed and the attempt is successful.
- the **Send Untranslated ARP** parameter in the General tab of the Configuration page can be
  - disabled, so that the AP will overwrite the MAC address in Address Resolution Protocol (ARP) packets before forwarding them.
  - enabled, so that the AP will forward ARP packets regardless of whether it has overwritten the MAC address.

This is the **Translation Bridging** feature, which you can enable in the General tab of the Configuration web page in the AP. When this feature is disabled, the setting of the **Send Untranslated ARP** parameter has no effect, because all packets are forwarded untranslated (with the source MAC address intact).

See Address Resolution Protocol on Page 164.

Chapter 14: Engineering VLANs

The radios support VLAN functionality as defined in the 802.1Q (*Virtual LANs*) specification, except for the following aspects of that specification:

- the following protocols:
  - Generic Attribute Registration Protocol (GARP) GARV
  - Spanning Tree Protocol (STP)
  - Multiple Spanning Tree Protocol (MSTP)
  - GARP Multicast Registration Protocol (GMRP)
- priority encoding (802.1P) before Release 7.0
- embedded source routing (ERIF) in the 802.1Q header
- multicast pruning
- flooding unknown unicast frames in the downlink

As an additional exception, the AP *does not* flood downward the unknown unicast frames to the SM.

A VLAN configuration in Layer 2 establishes a logical group within the network. Each computer in the VLAN, regardless of initial or eventual physical location, has access to the same data. For the network operator, this provides flexibility in network segmentation, simpler management, and enhanced security.

Special Case VLAN Numbers

This system handles special case VLAN numbers according to IEEE specifications:

VLAN Number	Purpose	Usage Constraint
0	These packets have 802.1p priority, but are otherwise handled as untagged.	Should not be used as a management VLAN.
1	Although not noted as special case by IEEE specifications, these packets identify traffic that was untagged upon ingress into the SM and should remain untagged upon egress. This policy is hard-coded in the AP.	Should not be used for system VLAN traffic.
4095	This VLAN is reserved for internal use.	Should not be used at all.

SM Membership in VLANs

With the supported VLAN functionality, the radios determine bridge forwarding on the basis of not only the destination MAC address, but also the VLAN ID of the destination. This provides flexibility in how SMs are used:

- Each SM can be a member in its own VLAN.
- Each SM can be in its own broadcast domain, such that only the radios that are members of the VLAN can see broadcast and multicast traffic to and from the SM.
- The network operator can define a work group of SMs, regardless of the AP(s) to which they register.

PMP modules provide the VLAN frame filters that are described in Table 41.

Table 41: VLAN filters in point-to-multipoint modules

Where VLAN is active, if this parameter value is selected …	**then a frame is discarded if… *entering* the bridge/ NAT switch through…**		**because of this VLAN filter in the software:**
	Ethernet…	**TCP/IP…**	
any combination of VLAN parameter settings	with a VID not in the membership table		Ingress
any combination of VLAN parameter settings		with a VID not in the membership table	Local Ingress
Allow Frame Types: Tagged Frames Only	with no 802.1Q tag		Only Tagged
Allow Frame Types: Untagged Frames Only	with an 802.1Q tag, regardless of VID		Only Untagged
Local SM Management: Disable in the SM, or **All Local SM Management: Disable** in the AP	with an 802.1Q tag and a VID in the membership table		Local SM Management
	***leaving* the bridge/ NAT switch through…**		
	Ethernet…	**TCP/IP…**	
any combination of VLAN parameter settings	with a VID not in the membership table		Egress
any combination of VLAN parameter settings		with a VID not in the membership table	Local Egress

Priority on VLANs (802.1p)

The radios can prioritize traffic based on the eight priorities described in the IEEE 802.1p specification. When the high-priority channel is enabled on an SM, regardless of whether VLAN is enabled on the AP for the sector, packets received with a priority of 4 through 7 in the 802.1p field are forwarded onto the high-priority channel.

VLAN settings can also cause the module to convert received non-VLAN packets into VLAN packets. In this case, the 802.1p priority in packets leaving the module is set to the priority established by the DiffServ configuration.

If you enable VLAN, *immediately* monitor traffic to ensure that the results are as desired. For example, high-priority traffic may block low-priority.

For more information on the high priority channel, see High-priority Bandwidth on Page 86.

Q-in-Q DVLAN (Double-VLAN) Tagging (802.1AD)

PMP and PTP modules can be configured with 802.1ad Q-in-Q DVLAN (Double-VLAN) tagging which is a way for an operator to put an 802.1Q VLAN inside of an 802.1ad VLAN. A nested VLAN, which is the original 802.1Q tag and a new second 802.1ad tag, allows for bridging of VLAN traffic across a network and segregates the broadcast domains of 802.1Q VLANs. Q-in-Q can be used with PPPoE and/or NAT.

The 802.1ad standard defines the S-VLAN as the Service Provider VLAN and the C-VLAN as the customer VLAN. The radio software does 2 layer Q-in-Q whereby the C-VLAN is the 802.1Q tag and the S-VLAN is the second layer Q tag as shown in Table 42.

Table 42: Q-in-Q Ethernet frame

Ethernet Header	S-VLAN EthType 0x88a8	C-VLAN EthType 0x8100	IP Data EthType 0x0800

The 802.1ad S-VLAN is the outer VLAN that is configurable on the Configuration => VLAN web page of the AP and BHM. The Q-in-Q EtherType parameter is configured with a default EtherType of 0x88a8 in addition to four alternate EtherType's that can be configured to aid in interoperability with existing networks that use a different EtherType than the default.

The C-VLAN is the inner VLAN tag, which is the same as 802.1Q. As a top level concept, this operates on the outermost tag at any given time, either "pushing" a tag on or "popping" a tag off. This means packets will at most transition from an 802.1Q frame to an 801.ad frame (with a tag "pushed" on) or an untagged 802.1 frame (with the tag "popped" off. Similarly, for an 802.1ad frame, this can only transition from an 802.1ad frame to an 802.1Q frame (with the tag "popped" off) since the radio software only supports 2 levels of tags.

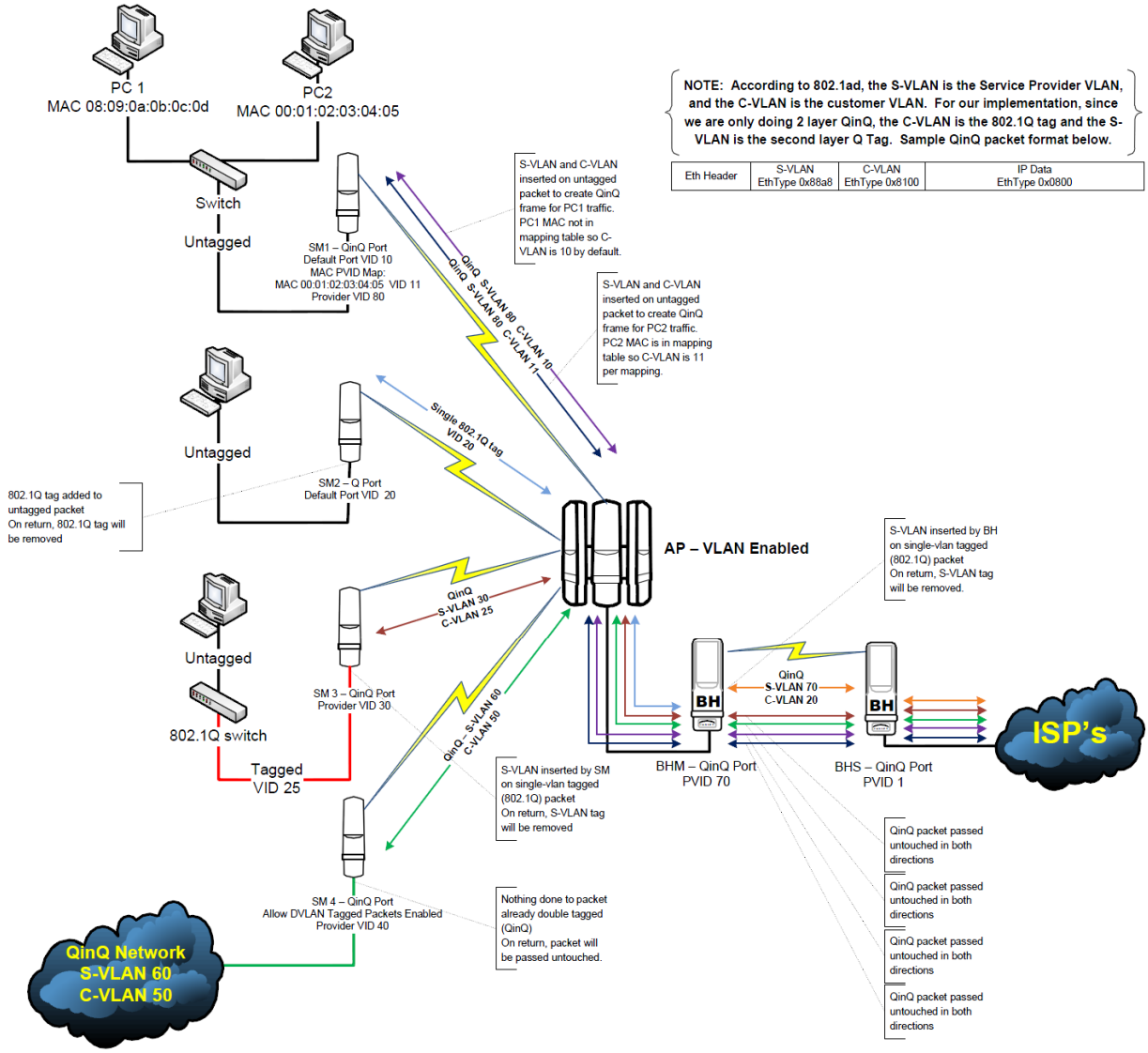

PC 1
MAC 08:09:0a:0b:0c:0d
PC2
MAC 00:01:02:03:04:05
NOTE: According to 802.1ad, the S-VLAN is the Service Provider VLAN, and the C-VLAN is the customer VLAN. For our implementation, since we are only doing 2 layer QinQ, the C-VLAN is the 802.1Q tag and the S-VLAN is the second layer Q Tag. Sample QinQ packet format below.
Eth Header
S-VLAN EthType 0x88a8
C-VLAN EthType 0x8100
IP Data EthType 0x0800
Switch
Untagged
SM1 – QinQ Port
Default Port VID 10
MAC PVID Map:
MAC 00:01:02:03:04:05 VID 11
Provider VID 80
S-VLAN and C-VLAN inserted on untagged packet to create QinQ frame for PC1 traffic. PC1 MAC not in mapping table so C-VLAN is 10 by default.
QinQ S-VLAN 80 C-VLAN 10
QinQ S-VLAN 80 C-VLAN 11
S-VLAN and C-VLAN inserted on untagged packet to create QinQ frame for PC2 traffic. PC2 MAC is in mapping table so C-VLAN is 11 per mapping.
Untagged
Single 802.1Q tag VID 20
SM2 – Q Port
Default Port VID 20
802.1Q tag added to untagged packet
On return, 802.1Q tag will be removed
AP – VLAN Enabled
S-VLAN inserted by BH on single-vlan tagged (802.1Q) packet
On return, S-VLAN tag will be removed.
Untagged
QinQ S-VLAN 30 C-VLAN 25
SM 3 – QinQ Port
Provider VID 30
802.1Q switch
Tagged VID 25
QinQ S-VLAN 60 C-VLAN 50
BH
BH
QinQ S-VLAN 70 C-VLAN 20
BHM – QinQ Port PVID 70
BHS – QinQ Port PVID 1
ISP's
S-VLAN inserted by SM on single-vlan tagged (802.1Q) packet
On return, S-VLAN tag will be removed
QinQ packet passed untouched in both directions
QinQ packet passed untouched in both directions
QinQ packet passed untouched in both directions
QinQ packet passed untouched in both directions
SM 4 – QinQ Port
Allow DVLAN Tagged Packets Enabled
Provider VID 40
Nothing done to packet already double tagged (QinQ)
On return, packet will be passed untouched.
QinQ Network
S-VLAN 60
C-VLAN 50

Figure 54 Q-in-Q network diagram

In this diagram, we have four example PMP SM endpoints and a BH pair that are using VLAN configurations involving Q-in-Q. For Multipoint and Point-to-Point systems, the VLAN Port type can be configured to be one of two modes: Q or Q-in-Q.

- For Q mode, this means the port will operate just like today's existing VLAN implementation. It will not add a second layer S-Tag, but it will add and remove the regular Q-Tag.
- For Q-in-Q mode, there is a difference between the multipoint mode and the point to point mode. For Multipoint, an SM will be able to add 2 layers of tags to an untagged packet. It will also be able to just add the single outer S-Tag to an already-tagged 802.1Q packet.

Either way, once the packet leaves the AP, it will be a Q-in-Q frame. For Point-to-Point, it is a little bit different in that the Backhaul will never add 2 layers of tags to an untagged frame. It will only add one layer of tag, thus making the frame either a single 802.1Q tagged packet (for untagged packets), or an 802.1ad doubly-tagged frame for already tagged packets. You can think of it in this way: the backhaul will only ever add or remove one tag layer, the outermost tag. The multipoint SM can add or remove 2, 1, or 0 tags, depending on the packet type and the configuration. In the upper right of Figure 54 there is an example packet format showing both tags in place in a Q-in-Q frame.

SM1, on the top left of Figure 54, has its VLAN port configured as a Q-in-Q port and also has a single MAC address VID mapping. For this configuration, the Provider VID, which will be the outer S-Tag VID, is 80, the Default Port VID, which will be the inner C-Tag VID for devices not found in the MAC address mapping table, is 10, and finally, the single entry in the MAC-VID mapping table is VID 11 corresponding to MAC address 00:01:02:03:04:05. Underneath the SM, there are two PC devices. PC2 has a MAC address that is contained in the MAC address VID table mapping. So, for PC2, its effective Port VID will be 11, from the table. For PC1, since it is not in the table, it will use the Default Port VID which is 10. Once the untagged packets go through the SM and out of the AP, they will now be Q-in-Q frames with S-Tag VID of 80 and inner C-Tag VIDs of 10 for PC1 traffic, and 11 for PC2 traffic. These flows will then go across the Backhaul pair with no modifications to and from the ISP network.

SM2, second from top left in Figure 54 is receiving and sending untagged packets to the client PC underneath of it. SM has a Default Port VID (Untagged Ingress VID) of 20 and is configured as a Q VLAN Port type. So, when a packet comes in from the PC and goes out the AP, it will be an 802.1Q tagged packet with VID of 20. On the return path, the SM will strip the Q tag and send the untagged packet to the PC.

SM3, second from bottom left in Figure 54, has a client PC underneath of it with an 802.1Q switch in between that is tagging and untagging traffic from the PC. This switch is putting PC traffic onto 802.1Q VID 25. The SM is configured with a Q-in-Q VLAN Port Type with a Default Port VID of 30. So, when the packet leaves the SM and comes out of the AP, it will be an 802.1ad Q-in-Q packet with S-Tag VID of 30 and C-Tag VID of 25. On the return path, the 802.1ad Q-in-Q packet will have its S-Tag stripped and the resulting 802.1Q packet with VID of 25 will be sent down to the switch where it will be further stripped to an untagged packet.

SM4, bottom left in Figure 54, has an existing 802.1ad Q-in-Q network below it, meaning that packets coming into the SM's Ethernet interface are already doubly tagged 802.1ad frames. These frames have an S-Tag VID of 60 and a C-Tag VID of 50. The SM is configured with a Q-in-Q VLAN Port Type with a Provider VID of 40. If the Provider VID were the same as the underlying network S-Tag VID (60), then it would not work because the SM would be stripping the outer tag on the return path. Therefore, in this case, it is important that the SM's Provider VID does NOT match the S-Tag VID of the Q-in-Q network underneath. In this case, the 802.1ad frames are passed through untouched above and below the SM.

For the BH units, they must be configured as a Q-in-Q VLAN Port Type if they are to add and remove S-Tags. In this case, both sides are configured as Q-in-Q Port Types with the BHM having a Provider VID of 70 and the BHS having a Provider VID of 1. The packet flows shown in Figure 54 show that all but one of them are already 802.1ad Q-in-Q frames when they reach the BHM in the upstream direction. There is one stream that is a single 802.1Q tagged packet. For this stream, the BHM will add an S-Tag to it with Provider VID of 70, turning it into an 802.1ad frame. Since the BHS has Provider VID of 1, it will not add or remove any tag layers. As is the case with regular VLANs, VID of 1 is a special case in the Canopy network. At this point, all of the packet streams are Q-in-Q frames going into the ISP network. On the return path, Figure 54 shows where the tags are removed. One stream will have its S-Tag removed by the BHM in the downstream direction since its S-Tag VID matches the BHM Provider VID. Other streams will have their tags removed by other devices:

- SM1 will remove both S-Tag and C-Tag leaving an untagged packet for PC1 and PC2.
- SM2 will remove the Q-Tag (its S-Tag was removed by the BHM) from the stream, leaving an untagged packet for its PC.
- SM3 will remove the S-Tag, leaving the 802.1Q tagged frame for the 802.1Q switch handle for its PC.
- SM4 will not remove any tags, as it will be sending the 802.1ad frames into the Q-in-Q network underneath.

In the Figure 54 example above, the S-Tag EtherType is the default 0x88a8 which is specified by the 802.1ad specification. In order to accommodate interoperability, you may configure a different EtherType for Q-in-Q packets. This can only be configured on the AP for Multipoint systems, or the Backhaul Master for point-to-point systems. Once configured on these devices, it will be passed down to the SMs, or Backhaul Slave, so that both sides of the link will be using the same EtherType.

Installation and Configuration Guide

Chapter 15: Avoiding Hazards

Use simple precautions to protect staff and equipment. Hazards include exposure to RF waves, lightning strikes, and power surges. This section specifically recommends actions to abate these hazards.

Exposure Separation Distances

To protect from overexposure to RF energy, install the radios so as to provide and maintain the minimum separation distances shown in Table 43 away from all persons.

Table 43: Exposure separation distances

Module Type	Minimum Separation Distance from Persons
FSK or OFDM module	20 cm (approx 8 in)
Module with Reflector Dish	1.5 m (approx 60 in or 5 ft)
Module with LENS	0.5 m (approx 20 in)
Antenna of connectorized 5.7-GHz AP	30 cm (approx 12 in)
Antenna of connectorized or integrated 900-MHz module	60 cm (24 in)
Indoor 900-MHz SM	10 cm (4 in)

At these and greater separation distances, the power density from the RF field is below generally accepted limits for the general population.

NOTE:
These are conservative distances that include compliance margins. In the case of the reflector, the distance is even more conservative because the equation models the reflector as a point source and ignores its physical dimensions.

Section Appendix and Table 44 give details and discussion of the associated calculations.

Details of Exposure Separation Distances Calculations and Power Compliance Margins

Limits and guidelines for RF exposure come from:

- US FCC limits for the general population. See the FCC web site at http://www.fcc.gov, and the policies, guidelines, and requirements in Part 1 of Title 47 of the Code of Federal Regulations, as well as the guidelines and suggestions for evaluating compliance in FCC OET Bulletin 65.
- Health Canada limits for the general population. See the Health Canada web site at http://www.hc-sc.gc.ca/rpb and Safety Code 6.
- ICNIRP (International Commission on Non-Ionizing Radiation Protection) guidelines for the general public. See the ICNIRP web site at http://www.icnirp.de/ and Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields.

The applicable power density exposure limits from the documents referenced above are

- 6 W/m^2 for RF energy in the 900-MHz frequency band in the US and Canada.
- 10 W/m^2 for RF energy in the 2.4-, 5.2-, 5.4-, and 5.7-GHz frequency bands.

Peak power density in the far field of a radio frequency point source is calculated as follows:

$$S = \frac{P \cdot G}{4 \pi d^2}$$

where
S = power density in W/m^2
P = RMS transmit power capability of the radio, in W
G = total Tx gain as a factor, converted from dB
d = distance from point source, in m

Rearranging terms to solve for distance yields $$d = \sqrt{\frac{P \cdot G}{4 \pi S}}$$

Table 44 shows calculated minimum separation distances *d*, recommended distances and resulting power compliance margins for each frequency band and antenna combination.

Table 44: Calculated exposure distances and power compliance margins

Band Range	Antenna	Variable			*d* (calculated)	Recommended Separation Distance	Power Compliance Margin
		P	***G***	**S**			
900 MHz	external	0.4 W (26 dBm)	10.0 (10 dB)	6 W/m^2	23 cm	60 cm (24 in)	7
	integrated	0.25 W (24 dBm)	15.8 (12 dB)	6 W/m^2	23 cm	60 cm (24 in)	7
	indoor, integrated	Simulation model used to estimate Specific Absorption Rate (SAR) levels				10 cm (4 in)	2
2.4 GHz	external	0.2 W (23 dBm)	19 W (13 dB)	10 W/m^2	17 cm	60 cm (24 in)	11.9
	integrated	0.34 W (25 dBm)	6.3 (8 dB)	10 W/m^2	13 cm	20 cm (8 in)	2.3
	integrated plus reflector	0.34 W (25 dBm)	79.4 (19 dB)	10 W/m^2	46 cm	1.5 m (5 ft)	10
5.2 GHz	integrated	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m^2	9 cm	20 cm (8 in)	5
	integrated plus reflector	0.0032 W (5 dBm)	316 (25 dB)	10 W/m^2	9 cm	1.5 m (5 ft)	279
	integrated plus LENS	0.025 W (14 dBm)	40 (16 dB)	10 W/m^2	9 cm	50 cm (12 in)	31
5.4 GHz	integrated	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m^2	9 cm	20 cm (8 in)	5
	integrated plus reflector	0.0032 W (5 dBm)	316 (25 dB)	10 W/m^2	9 cm	1.5 m (5 ft)	279
	integrated plus LENS	0.020 W (13 dBm)	50 (17 dB)	10 W/m^2	9 cm	50 cm (12 in)	31
5.4 GHz OFDM	integrated	0.01 W (10 dBm)	50 (17 dB)	10 W/m^2	6 cm	20 cm (8 in)	10
5.7 GHz	External	0.2 W (23 dBm)	19 W (13 dB)	10 W/m^2	17 cm	60 cm (24 in)	11.9
	integrated	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m^2	9 cm	20 cm (8 in)	5
	integrated plus reflector	0.2 W (23 dBm)	316 (25 dB)	10 W/m^2	71 cm	1.5 m (5 ft)	4.5
	integrated plus LENS	0.2 W (23 dBm)	50 (17 dB)	10 W/m^2	28 cm	50 cm (12 in)	3.13

The Recommended Separation Distance provides significant compliance margin in all cases. To simplify exposure distances in this column, a module has the expressed separation distance regardless of whether it is retrofitted with a reflector or a LENS.

These are conservative distances:

- They are along the beam direction (the direction of greatest energy). Exposure to the sides and back of the module is significantly less.
- They satisfy sustained exposure limits for the general population (not just short term occupational exposure limits), with considerable margin.
- In the reflector cases, the calculated compliance distance *d* is greatly overestimated because the far-field equation models the reflector as a point source and neglects the physical dimension of the reflector.

Grounding the Equipment

Effective lightning protection diverts lightning current safely to ground, Protective Earth (PE) ⏚. It neither attracts nor prevents lightning strikes.

WARNING!

Lightning damage *is not* covered under the warranty. The recommendations in this guide give the installer the knowledge to protect the installation from the harmful effects of ESD and lightning.

These recommendations must be thoroughly and correctly performed. However, complete protection is neither implied or possible.

Grounding Infrastructure Equipment

To protect both your staff and your infrastructure equipment, implement lightning protection as follows:

- Observe all local and national codes that apply to grounding for lightning protection.
- Before you install your modules, perform the following steps:
  - Engage a grounding professional if you need to do so.
  - Install lightning arrestors to transport lightning strikes away from equipment. For example, install a lightning rod on a tower leg other than the leg to which you mount your module.
  - Connect your lightning rod to ground.
  - Use a 600SS Surge Suppressor on the Ethernet cable where the cable enters any structure. (Instructions for installing this surge suppressor are provided in Procedure 22 on Page 398.)
- Install your modules at least 2 feet (0.6 meters) below the tallest point on the tower, pole, or roof.

Grounding SMs

This section provides lightning protection guidelines for SMs to satisfy the National Electrical Code (NEC) of the United States. The requirements of the NEC focus on the safety aspects of electrical shock to personnel and on minimizing the risk of fire at a dwelling. The NEC does not address the survivability of electronic products that are exposed to lightning surges.

The statistical incidence of current levels from lightning strikes is summarized in Table 45.

Table 45: Statistical incidence of current from lightning strikes

Percentage of all strikes	Peak Current (amps)
<2	>140,000
25	>35,000
>50	>20,000
>80	>8,500

At peak, more than one-half of all surges due to direct lightning strikes exceed 20,000 amps. However, only one-quarter exceed 35,000 amps, and less than two percent exceed 140,000 amps. Thus, the recommended Surge Suppressor provides a degree of lightning protection to electronic devices inside a dwelling.

Summary of Grounding Recommendations

Cambium recommends that you ground each SM as follows:

- Extend the SM mounting bracket extend to the top of the SM or higher.
- Ground the SM mounting bracket via a 10-AWG (6 mm^2) copper wire connected by the most direct path either to an eight foot-deep ground rod or to the ground bonding point of the AC power service utility entry. This provides the best assurance that
  - lightning takes the ground wire route
  - the ground wire does not fuse open
  - your grounding system complies with NEC 810-15.
- Ground the surge suppressor ground lug to the same ground bonding point as above, using at least a 10-AWG (6 mm^2) copper wire. This provides the best assurance that your grounding system complies with NEC 810-21.

Grounding Scheme

The proper overall antenna grounding scheme per the NEC is illustrated in Figure 136 on Page 399. In most television antenna or dish installations, a coaxial cable connects the outdoor electronics with the indoor electronics. To meet NEC 810-20, one typically uses a coaxial cable feed-through block that connects the outdoor coax to the indoor coax and also has a screw for attaching a ground wire. This effectively grounds the outer shield of the coax. The block should be mounted on the outside of the building near the AC main panel such that the ground wire of the block can be bonded to the primary grounding electrode system of the structure.

For residential installs, in most cases an outdoor rated *un*shielded twisted pair (UTP) cable is sufficient. To comply with the NEC, Cambium provides the antenna discharge unit, 600SS, for each conductor of the cable. The surge suppressor must be

- positioned
  - outside the building.
  - as near as practicable to the power service entry panel of the building and attached to the AC main power ground electrode, or attached to a grounded water pipe.[5]
  - far from combustible material.
- grounded in accordance with NEC 810-21, with the grounding wire attached to the screw terminal.

The metal structural elements of the antenna mast also require a separate grounding conductor. Section 810-15 of the NEC states:

> *Masts and metal structures supporting antennas shall be grounded in accordance with Section 810-21.*

As shown in Figure 136 on Page 399, the Cambium recommendation for grounding the metal structural element of the mounting bracket (SMMB1) is to route the grounding wire from the SMMB1 down to the same ground attachment point as is used for the 600SS discharge unit.

Use 10-AWG (6 mm^2) Copper Grounding Wire

According to NEC 810-21 3(h), either a 16-AWG copper clad steel wire or a 10-AWG copper wire may be used. This specification appears to be based on mechanical strength considerations and *not* on lightning current handling capabilities.

For example, analysis shows that the two wire types are not equivalent when carrying a lightning surge that has a 1-microsecond rise by 65-microsecond fall:

- The 16-AWG copper clad steel wire has a peak fusing current of 35,000 amps and can carry 21,000 amps peak, at a temperature just below the ignition point for paper (454° F or 234° C).
- The 10-AWG copper wire has a peak fusing current of 220,000 amps and can carry 133,000 amps peak, at the same temperature.

[5] It is *insufficient* to merely use the green wire ground in a duplex electrical outlet box for grounding of the antenna discharge unit.

Based on the electrical/thermal analysis of these wires, Cambium recommends 10-AWG copper wire for *all* grounding conductors. Although roughly double the cost of 16-AWG copper clad steel wire, 10-AWG copper wire handles six times the surge current from lightning.

Shielding is not Grounding

In part, NEC 810-21 states:

> *A lightning arrester is not required if the lead-in conductors are enclosed in a continuous metal shield, such as rigid or intermediate metal conduit, electrical metallic tubing, or any metal raceway or metal-shielded cable that is effectively grounded. A lightning discharge will take the path of lower impedance and jump from the lead-in conductors to the metal raceway or shield rather than take the path through the antenna coil of the receiver.*

However, Cambium does not recommend relying on shielded twisted pair cable for lightning protection for the following reasons:

- Braid-shielded 10Base-T cable is uncommon, if existent, and may be unsuitable anyway.
- At a cost of about two-thirds more than 10-AWG copper UTP, CAT 5 100Base-TX foil-shielded twisted pair (FTP) cable provides a 24-AWG drain wire. If this wire melts open during a lightning surge, then the current may follow the twisted pair into the building.

More than 80 percent of all direct lightning strikes have current that exceeds 8,500 amps (see Table 45 on Page 178). A 24-AWG copper wire melts open at 8,500 amps from a surge that has a 1-microsecond by 70-microsecond waveform. Hence, reliance on 24-AWG drain wire to comply with the intent of NEC 810-21 is questionable.

Shielded twisted pair cable may be useful for mitigation of interference in some circumstances, but installing surge suppressors and implementing the ground recommendations constitute the most effective mitigation against lightning damage.

Grounding PMP 400 SMs

PMP 54400 APs and SMs and PTP 54200 BHs use a nominal 30-V DC power system with power on Pins 7 and 8 and return on Pins 4 and 5. PMP 54400 APs and PTP 54200 BHs can be powered from either a CMMmicro with a 30-V DC power supply or a CMM4 with a 30-V DC power supply. A 29.5-V DC power supply is available for PMP 54400 SMs.

In contrast, PMP 49400 APs and SMs and PTP 49200 BHs use a nominal 56-V DC power system with power on Pins 5 and 8 and return on Pins 4 and 7. PMP 49400 APs and PTP 49200 BHs *must* use a CMM4 with a 56-V DC power supply. A CMMmicro *will not* power these units, because it provides the wrong voltage on the wrong pins. A 56-V DC power supply is available for PMP 49400 SMs.

IMPORTANT!

When working on sites with both power systems, use care to not wrongly mix power supplies and radios, because the two power systems use different pinout schemes and require different voltages.

On a site where you are deploying a mix of 30-V DC and 56-V DC radios (to the limit of 8 radios supported by one CMM), you can use a CMM4 that is connected to both a 30-V DC power supply and a 56-V DC power supply.

Due to the full metallic connection to the tower or support structure through the AP antenna or a connectorized BH antenna, grounding the AP or BH and installing a 600SS surge suppressor within 3 ft (1 m) of the AP or BH is *strongly recommended.* This suppresses overvoltages and overcurrents, such as those caused by near-miss lightning. APs and BHs provide a grounding lug for grounding to the tower or support structure. A pole mount kit is available for the 600SS. The pole mount kit provides a grounding point on one of its U-bolts that can be used for terminating ground straps from both the 600SS and the AP.

NEC Reference

NEC Article 810, *Radio and Television Equipment*, and associated documents and discussions are available from http://www.neccode.com/index.php?id=homegeneral, http://www.constructionbook.com/xq/ASP/national-electrical-code-2005/id.370/subID.746/qx/default2.htm, and other sources.

Conforming to Regulations

For all electrical purposes, ensure that your network conforms to applicable country and local codes, such as the NEC (National Electrical Code) in the US. If you are uncertain of code requirements, engage the services of a licensed electrician.

Protecting Cables and Connections

Cables that move in the wind can be damaged, impart vibrations to the connected device, or both. At installation time, prevent these problems by securing all cables with cable ties, cleats, or PVC tape.

Over time, moisture can cause a cable connector to fail. You can prevent this problem by

- using cables that are filled with a dielectric gel or grease.
- including a drip loop where the cable approach to the module (typically a CMM) is from above.
- wrapping the cable with weather-resistant tape.

On a module with an external antenna, use accepted industry practices to wrap the connector to prevent water ingress. Although the male and female N-type connectors form a gas-tight seal with each other, the point where the cable enters each connector can allow water ingress and eventual corrosion. Wrapping and sealing is critical to long-term reliability of the connection.

Possible sources of material to seal that point include

- the antenna manufacturer (material may have been provided in the package with the antenna).
- Universal Electronics (whose web site is http://www.coaxseal.com), who markets a weather-tight wrap named Coax-Seal.

Perform the following steps to wrap the cable.

Procedure 4: Wrapping the cable

1. Start the wrap on the cable 0.5 to 2 inches (about 1.5 to 5 cm) from the connection.
2. Wrap the cable to a point 0.5 to 2 inches (about 1.5 to 5 cm) above the connection.
3. Squeeze the wrap to compress and remove any trapped air.
4. Wrap premium vinyl electrical tape over the first wrap where desired for abrasion resistance or appearance.
5. Tie the cable to minimize sway from wind.

Chapter 16: Testing the Components

The best practice is to connect all components—BHs, APs, GPS antenna, and CMM—in a test setting and initially configure and verify them before deploying them to an installation. In this way, any configuration issues are worked out before going on-site, on a tower, in the weather, where the discovery of configuration issues or marginal hardware is more problematic and work-flow affecting.

Unpacking Components

When you receive these products, carefully inspect all shipping boxes for signs of damage. If you find damage, immediately notify the transportation company.

As you unpack the equipment, verify that all the components that you ordered have arrived. Save all the packing materials to use later, as you transport the equipment to and from installation sites.

Configuring for Test

You can use either of two methods to configure an AP or BHM:

- Use the Quick Start feature of the product. For more information on Quick Start, see Quick Start Page of the AP on Page 191.
- Manually set each parameter.

After you change configuration parameters on a GUI web page:

- Before you leave a web page, click the **Save** button to save the change(s).
- After making change(s) on multiple web pages, click the **Reboot** button to reboot the module and implement the change(s).

Configuring the Computing Device for Test

If your computer is configured for Dynamic Host Configuration Protocol (DHCP), disconnect the computer from the network. If your computer is instead configured for static IP addressing

- set the static address in the 169.254 network
- set the subnet mask to 255.255.0.0.

Default Module Configuration

From the factory, the AP, SM, and BH are all configured to *not transmit* on any frequency. This configuration ensures that you do not accidentally turn on an unsynchronized module. Site synchronization of modules is required because

- modules
  - cannot transmit and receive signals at the same time.
  - use TDD (Time Division Duplexing) to distribute signal access of the downlink and uplink frames.
- when one module transmits while an unintended module nearby receives signal, the transmitting module may interfere with or desense the receiving module. In this context, interference is self-interference (within the same network).

Component Layout

As shown in Figure 55, the base cover of the module snaps off when you depress a lever on the back of the base cover. This exposes the Ethernet and GPS sync connectors and diagnostic LEDs.

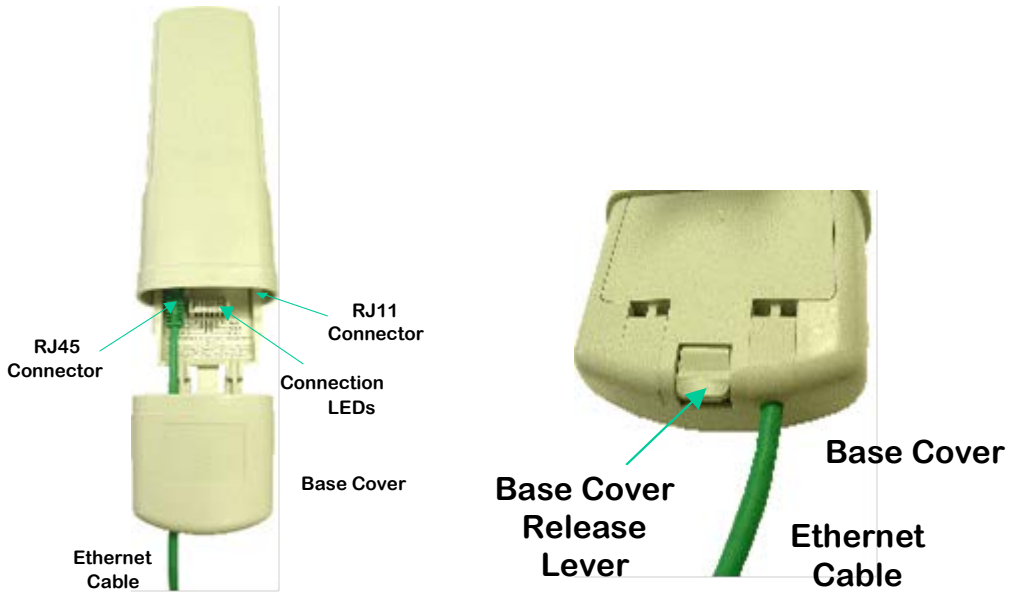


Figure 55: Base cover, detached and attached, FSK module

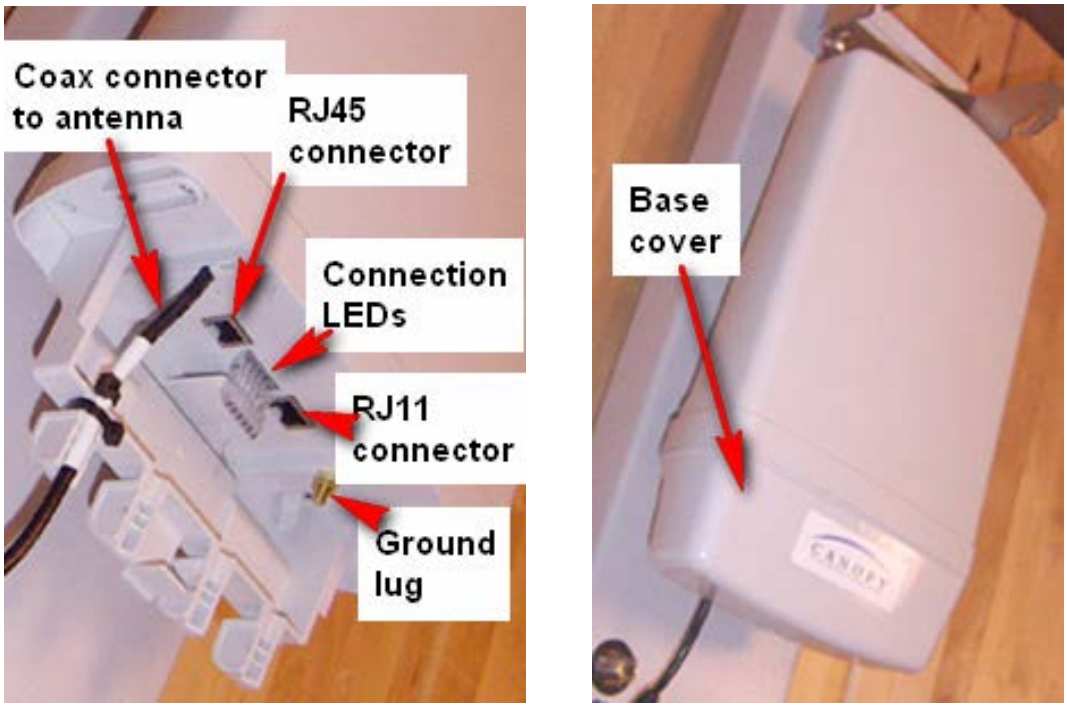


Figure 56: Base cover, detached and attached, OFDM module

Diagnostic LEDs

The diagnostic LEDs report the following information about the status of the module. Table 46 and Table 47 identify the LEDs in order of their left-to-right position as the cable connections face downward.

> ***NOTE:***
> The LED color helps you distinguish position of the LED. The LED color *does not* indicate any status.

Table 46: LEDs in AP and BHM

Label	Color when Active	Status Information Provided	Notes
LNK/5	green	Ethernet link	Continuously lit when link is present.
ACT/4	yellow	Presence of data activity on the Ethernet link	Flashes during data transfer. Frequency of flash is not a diagnostic indication.
GPS/3	red	Pulse of sync	Continuously lit as pulse as AP receives pulse.
SES/2	green	*Unused on the AP*	SES is the session indicator on the CMM.

Label	Color when Active	Status Information Provided	Notes
SYN/1	yellow	Presence of sync	Always lit on the AP.
PWR	red	DC power	Always lit when power is correctly supplied.

Table 47: Legacy Mode LEDs in SM and BHS

Label	Color when Active	Status if Registered	Notes	
			Operating Mode	Aiming Mode
LNK/5	green	Ethernet link	Continuously lit when link is present.	These five LEDs act as a bar graph to indicate the relative quality of alignment. As power level and jitter (if present) improve during alignment, more of these LEDs are lit.
ACT/4	yellow	Presence of data activity on the Ethernet link	Flashes during data transfer. Frequency of flash is not a diagnostic indication.	
GPS/3	red	*Unused*	If this module is not registered to another, then these three LEDs cycle on and off from left to right.	
SES/2	green	*Unused*		
SYN/1	yellow	Presence of sync		
PWR	red	DC power	Always lit when power is correctly supplied.	Always lit when power is correctly supplied.

An optional light scheme configurable in all FSK SMs supports end customers who install the SM (for example, the 9000SMQ indoor SM) on their own premises. The scheme uses the LEDs and labels listed in Table 47 above, but is based on the traffic signal light analogy: green is good, yellow is okay, and red is bad. This scheme can also be useful in some settings and workflows for outdoor SMs. As with Legacy mode, while the SM is scanning, the green, yellow, and red LEDs blink in sequence.

Table 48: Revised Mode LEDs in SM

Label	Color	Revised Mode Indication
LNK/5	green	*Link.*
ACT/4	yellow	*Activity.*
GPS/3	red	*Interference (Jitter)* On - high interference. Blinking - medium interference. Off - low interference.
SES/2	green	*Strong Receive Signal Power* Blinking from slow to full-on to indicate strong power, getting stronger.
SYN/1	yellow	*Medium Receive Signal Power* Blinking from slow to full-on to indicate medium power, getting stronger.

Label	Color	Revised Mode Indication
PWR	red	*Not Registered* Off when registered to AP. On when not registered to AP.

To configure an SM into the Revised Mode, see LED Panel Mode on Page 323.

Standards for Wiring

Modules automatically sense whether the Ethernet cable in a connection is wired as straight-through or crossover. You may use either straight-through or crossover cable to connect a network interface card (NIC), hub, router, or switch to these modules. For a straight-through cable, use the EIA/TIA-568B wire color-code standard on both ends. For a crossover cable, use the EIA/TIA-568B wire color-code standard on one end, and the EIA/TIA-568A wire color-code standard on the other end.

Where you use the AC wall adapter

- the power supply output is +24 VDC.
- the power input to the SM is +11.5 VDC to +30 VDC.
- the maximum Ethernet cable run is 328 feet (100 meters).

Best Practices for Cabling

The following practices are essential to the reliability and longevity of cabled connections:

- Use only shielded cables to resist interference.
- For vertical runs, provide cable support and strain relief.
- Include a 2-ft (0.6-m) service loop on each end of the cable to allow for thermal expansion and contraction and to facilitate terminating the cable again when needed.
- Include a drip loop to shed water so that most of the water does not reach the connector at the device.
- Properly crimp all connectors.
- Use dielectric grease on all connectors to resist corrosion.
- Use only shielded connectors to resist interference and corrosion.

Recommended Tools for Wiring Connectors

The following tools may be needed for cabling the AP:

- RJ-11 crimping tool
- RJ-45 crimping tool
- electrician scissors

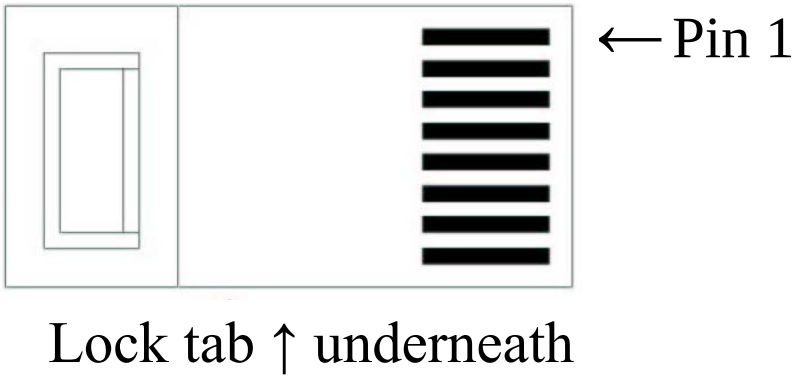
- wire cutters
- cable testing device

Wiring Connectors

The following diagrams correlate pins to wire colors and illustrate crossovers where applicable.

Location of Pin 1

Pin 1, relative to the lock tab on the connector of a straight-through cable is located as shown below.



RJ-45 Pinout for Straight-through Ethernet Cable

Pin 1 →	white / orange	← Pin 1
Pin 2 →	orange	← Pin 2
Pin 3 →	white / green	← Pin 3
Pin 4 →	blue	← Pin 4
Pin 5 →	white / blue	← Pin 5
Pin 6 →	green	← Pin 6
Pin 7 →	white / brown	← Pin 7
Pin 8 →	brown	← Pin 8

Pins 7 and 8 carry power to the modules.

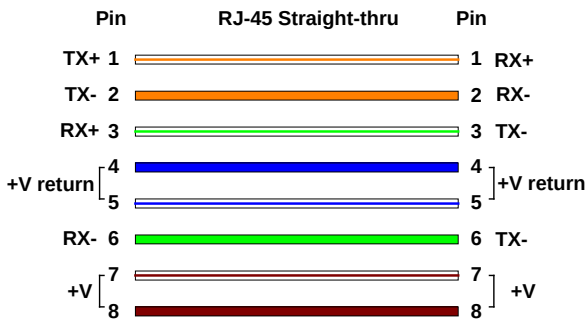


Figure 57: RJ-45 pinout for straight-through Ethernet cable

RJ-45 Pinout for Crossover Ethernet Cable

Pin 1 → white / orange ← Pin 3
Pin 2 → orange ← Pin 6
Pin 3 → white / green ← Pin 1
Pin 4 → blue ← Pin 4
Pin 5 → white / blue ← Pin 5
Pin 6 → green ← Pin 2
Pin 7 → white / brown ← Pin 7
Pin 8 → brown ← Pin 8
Pins 7 and 8 carry power to the modules.

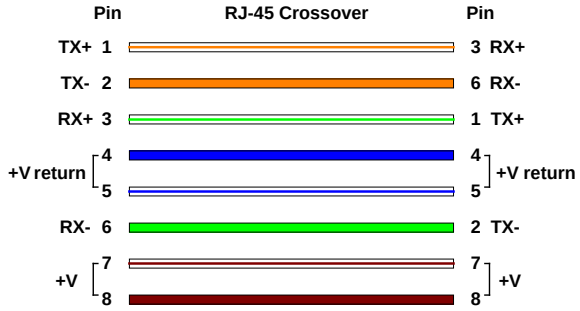


Figure 58: RJ-45 pinout for crossover Ethernet cable

RJ-11 Pinout for Straight-through Sync Cable

The system uses a utility cable with RJ-11 connectors between the AP or BH and synchronization pulse. Presuming CAT 5 cable and 6-pin RJ-11 connectors, the following diagram shows the wiring of the cable for sync.

Pin 1 → white / orange ← Pin 1
Pin 2 → white / green ← Pin 2
Pin 3 → white / blue ← Pin 3
Pin 4 → green ← Pin 4
Pin 5 → blue ← Pin 5
Pin 6 → orange ← Pin 6
NOTE: The fourth pair is not used.

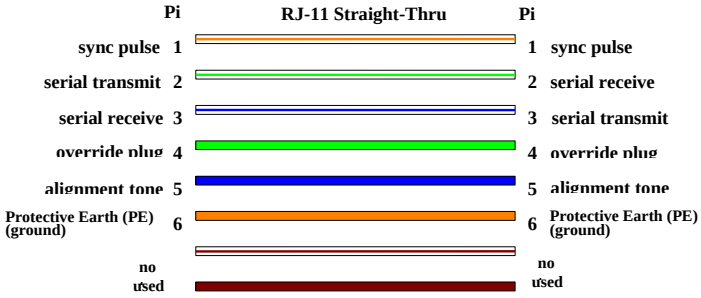


Figure 59: RJ-11 pinout for straight-through sync cable

Alignment Tone—Technical Details

The alignment tone output from a module is available on Pin 5 of the RJ-11 connector, and ground is available on Pin 6. Thus the load at the listening device should be between Pins 5 and 6. The listening device may be a headset, earpiece, or battery-powered speaker.

Configuring a Point-to-Multipoint Link for Test

Perform the following steps to begin the test setup.

Procedure 5: Setting up the AP for Quick Start

1. In one hand, securely hold the top (larger shell) of the AP. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
2. Plug one end of a CAT 5 Ethernet cable into the AP.
3. Plug the Ethernet cable connector labeled To Radio into the jack in the pig tail that hangs from the power supply.

WARNING!
From this point until you remove power from the AP, stay at least as far from the AP as the minimum separation distance specified in Table 43 on Page 174.

4. Plug the other connector of the pig tail (this connector labeled To Computer) into the Ethernet jack of the computing device.
5. Plug the power supply into an electrical outlet.
6. Power up the computing device.
7. Start the browser in the computing device.

The AP interface provides a series of web pages to configure and monitor the unit. You can access the web-based interface through a computing device that is either directly connected or connected through a network to the AP. If the computing device is not connected to a network when you are configuring the module in your test environment, and if the computer has used a proxy server address and port to configure a module, then you may need to first disable the proxy setting in the computer.

Perform the following procedure to toggle the computer to *not* use the proxy setting.

Procedure 6: Bypassing proxy settings to access module web pages

1. Launch Microsoft Internet Explorer.
2. Select **Tools→Internet Options→Connections→LAN Settings**.
3. Uncheck the **Use a proxy server…** box.
   NOTE: If you use an alternate web browser, the menu selections differ from the above.

In the address bar of your browser, enter the IP address of the AP. (For example, enter **`http://169.254.1.1`** to access the AP through its default IP address). The AP responds by opening the General Status tab of its Home page.

Quick Start Page of the AP

To proceed with the test setup, click the **Quick Start** button on the left side of the General Status tab. The AP responds by opening the Quick Start page. The Quick Start tab of that page is displayed in Figure 60.

NOTE:
If you cannot find the IP address of the AP, see Override Plug on Page 59.

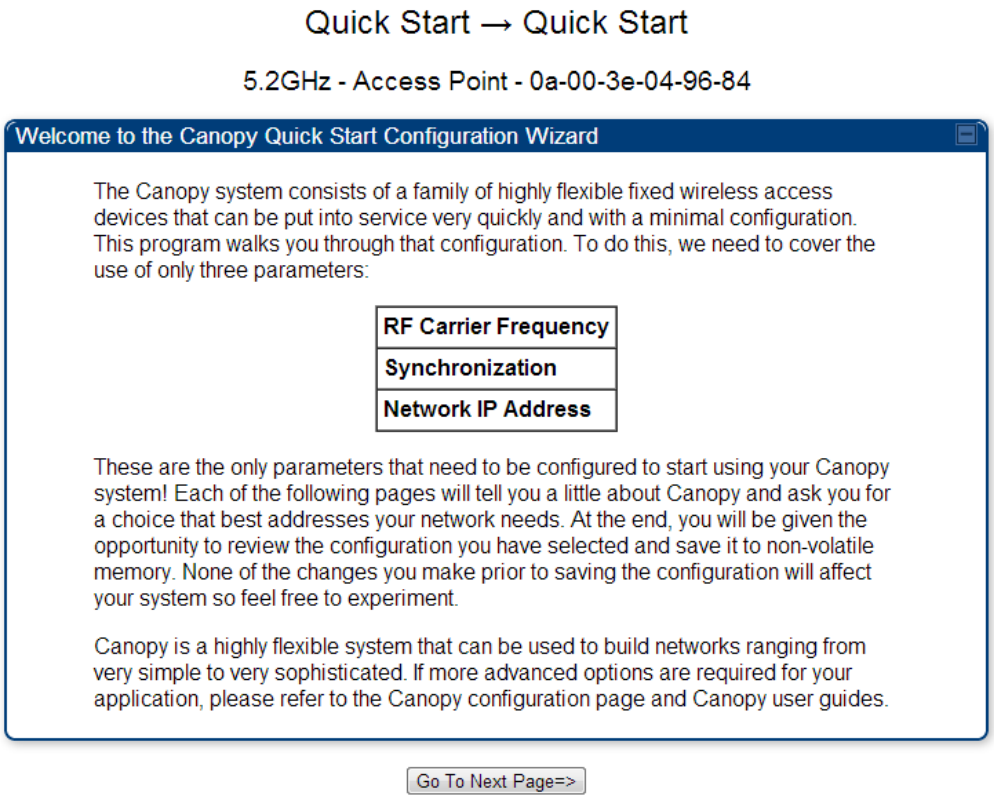

Quick Start → Quick Start
5.2GHz - Access Point - 0a-00-3e-04-96-84
Welcome to the Canopy Quick Start Configuration Wizard
The Canopy system consists of a family of highly flexible fixed wireless access devices that can be put into service very quickly and with a minimal configuration. This program walks you through that configuration. To do this, we need to cover the use of only three parameters:
RF Carrier Frequency
Synchronization
Network IP Address
These are the only parameters that need to be configured to start using your Canopy system! Each of the following pages will tell you a little about Canopy and ask you for a choice that best addresses your network needs. At the end, you will be given the opportunity to review the configuration you have selected and save it to non-volatile memory. None of the changes you make prior to saving the configuration will affect your system so feel free to experiment.
Canopy is a highly flexible system that can be used to build networks ranging from very simple to very sophisticated. If more advanced options are required for your application, please refer to the Canopy configuration page and Canopy user guides.
Go To Next Page=>

Figure 60: Quick Start tab of AP, example

Quick Start is a wizard that helps you to perform a basic configuration that places an AP into service. Only the following parameters must be configured:

- Region Code
- RF Carrier Frequency
- Synchronization
- LAN (Network) IP Address

In each Quick Start tab, you can

- specify the settings to satisfy the requirements of the network.
- review the configuration selected.
- save the configuration to non-volatile memory.

Proceed with the test setup as follows.

Procedure 7: Using Quick Start to configure a standalone AP for test

1. At the bottom of the Quick Start tab, click the **Go To Next Page =>** button.
   RESULT: The AP responds by opening the Region Settings tab. An example of this tab is shown in Figure 61.

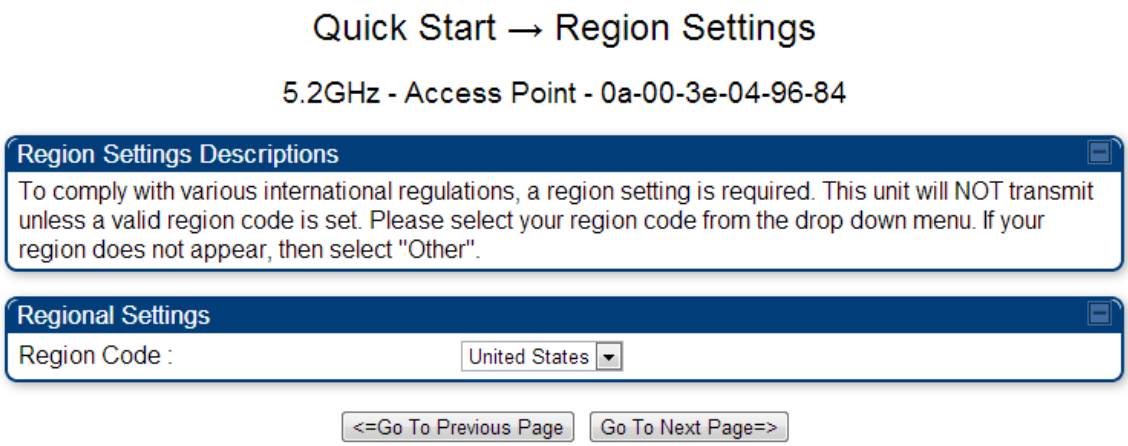

Quick Start → Region Settings
5.2GHz - Access Point - 0a-00-3e-04-96-84
Region Settings Descriptions
To comply with various international regulations, a region setting is required. This unit will NOT transmit unless a valid region code is set. Please select your region code from the drop down menu. If your region does not appear, then select "Other".
Regional Settings
Region Code :
United States
<=Go To Previous Page
Go To Next Page=>

Figure 61: Region Settings tab of AP, example

2. From the pull-down menu, select the region in which the AP will operate.

3. Click the **Go To Next Page =>** button.
   RESULT: The AP responds by opening the Radio Carrier Frequency tab. An example of this tab is shown in Figure 62.

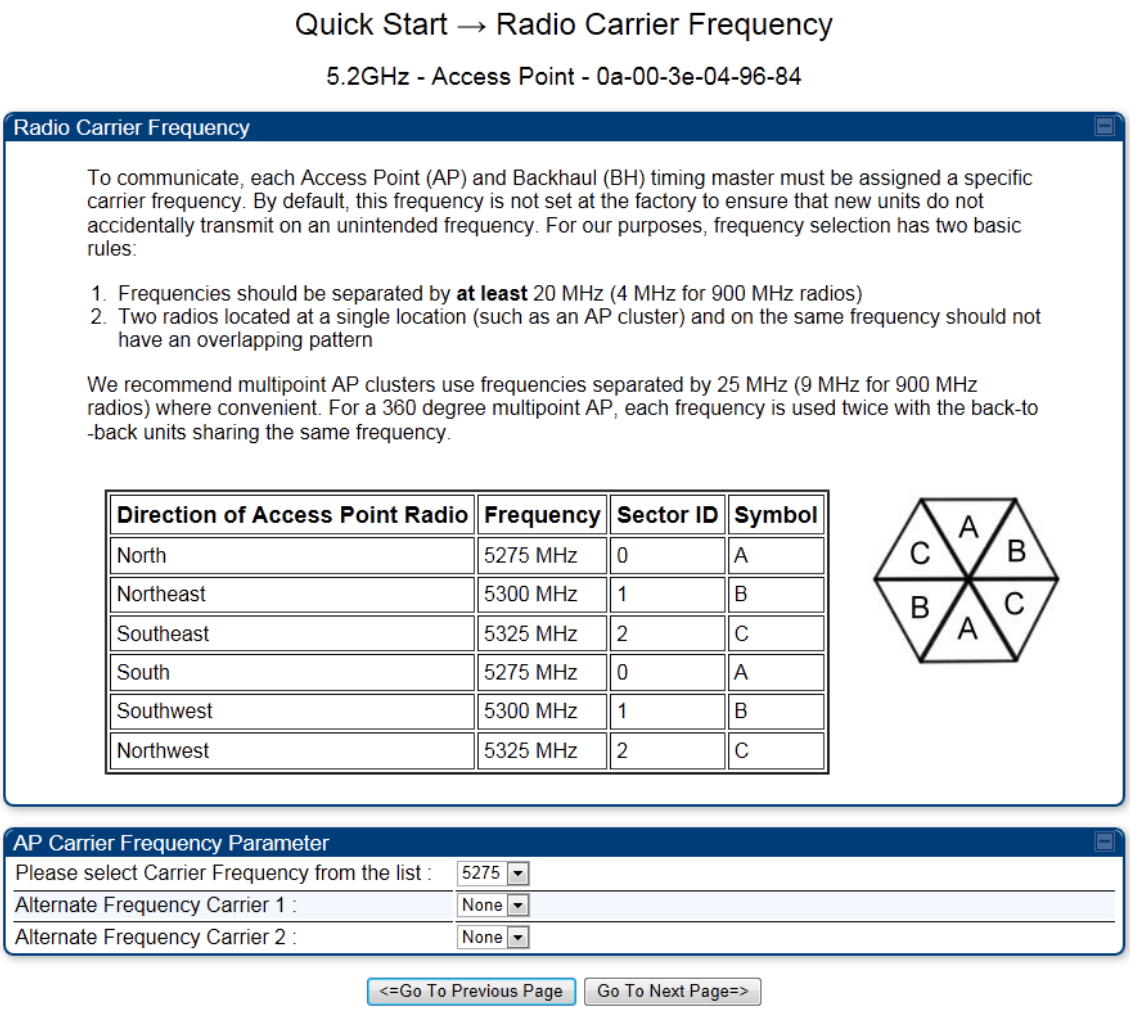

Quick Start → Radio Carrier Frequency
5.2GHz - Access Point - 0a-00-3e-04-96-84
Radio Carrier Frequency
To communicate, each Access Point (AP) and Backhaul (BH) timing master must be assigned a specific carrier frequency. By default, this frequency is not set at the factory to ensure that new units do not accidentally transmit on an unintended frequency. For our purposes, frequency selection has two basic rules:
1. Frequencies should be separated by at least 20 MHz (4 MHz for 900 MHz radios)
2. Two radios located at a single location (such as an AP cluster) and on the same frequency should not have an overlapping pattern
We recommend multipoint AP clusters use frequencies separated by 25 MHz (9 MHz for 900 MHz radios) where convenient. For a 360 degree multipoint AP, each frequency is used twice with the back-to-back units sharing the same frequency.
Direction of Access Point Radio | Frequency | Sector ID | Symbol
North | 5275 MHz | 0 | A
Northeast | 5300 MHz | 1 | B
Southeast | 5325 MHz | 2 | C
South | 5275 MHz | 0 | A
Southwest | 5300 MHz | 1 | B
Northwest | 5325 MHz | 2 | C
A
B
C
B
C
A
AP Carrier Frequency Parameter
Please select Carrier Frequency from the list : 5275
Alternate Frequency Carrier 1 : None
Alternate Frequency Carrier 2 : None
<=Go To Previous Page
Go To Next Page=>

Figure 62: Radio Carrier Frequency tab of AP, example

4. From the pull-down menu, select a frequency for the test.
5. Click the **Go To Next Page =>** button.
   RESULT: The AP responds by opening the Synchronization tab. An example of this tab is shown in Figure 63.

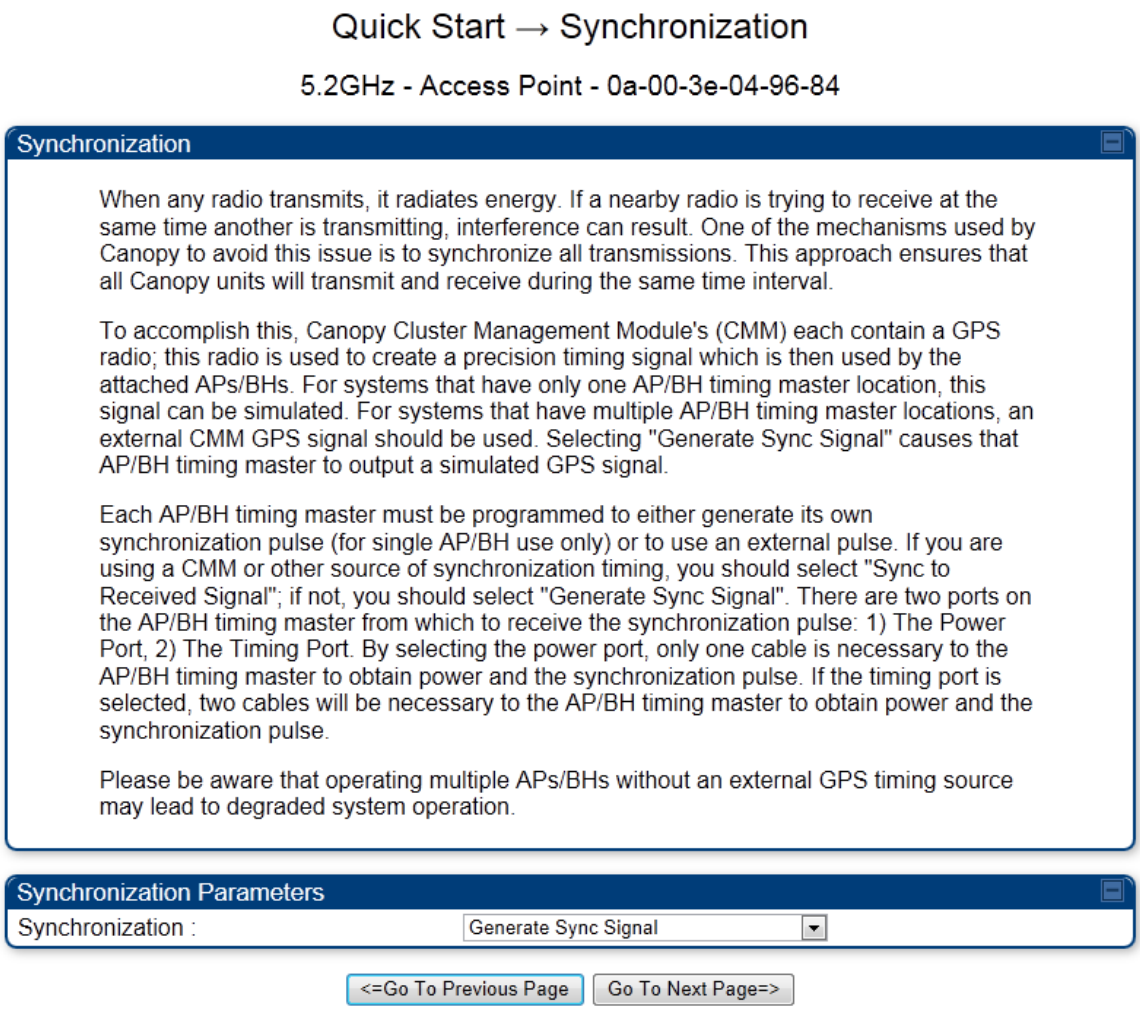

Quick Start → Synchronization
5.2GHz - Access Point - 0a-00-3e-04-96-84
Synchronization
When any radio transmits, it radiates energy. If a nearby radio is trying to receive at the same time another is transmitting, interference can result. One of the mechanisms used by Canopy to avoid this issue is to synchronize all transmissions. This approach ensures that all Canopy units will transmit and receive during the same time interval.
To accomplish this, Canopy Cluster Management Module's (CMM) each contain a GPS radio; this radio is used to create a precision timing signal which is then used by the attached APs/BHs. For systems that have only one AP/BH timing master location, this signal can be simulated. For systems that have multiple AP/BH timing master locations, an external CMM GPS signal should be used. Selecting "Generate Sync Signal" causes that AP/BH timing master to output a simulated GPS signal.
Each AP/BH timing master must be programmed to either generate its own synchronization pulse (for single AP/BH use only) or to use an external pulse. If you are using a CMM or other source of synchronization timing, you should select "Sync to Received Signal"; if not, you should select "Generate Sync Signal". There are two ports on the AP/BH timing master from which to receive the synchronization pulse: 1) The Power Port, 2) The Timing Port. By selecting the power port, only one cable is necessary to the AP/BH timing master to obtain power and the synchronization pulse. If the timing port is selected, two cables will be necessary to the AP/BH timing master to obtain power and the synchronization pulse.
Please be aware that operating multiple APs/BHs without an external GPS timing source may lead to degraded system operation.
Synchronization Parameters
Synchronization :
Generate Sync Signal
<=Go To Previous Page
Go To Next Page=>

Figure 63: Synchronization tab of AP, example

6. At the bottom of this tab, select **Generate Sync Signal**.
7. Click the **Go To Next Page =>** button.
   RESULT: The AP responds by opening the LAN IP Address tab. An example of this tab is shown in Figure 64.

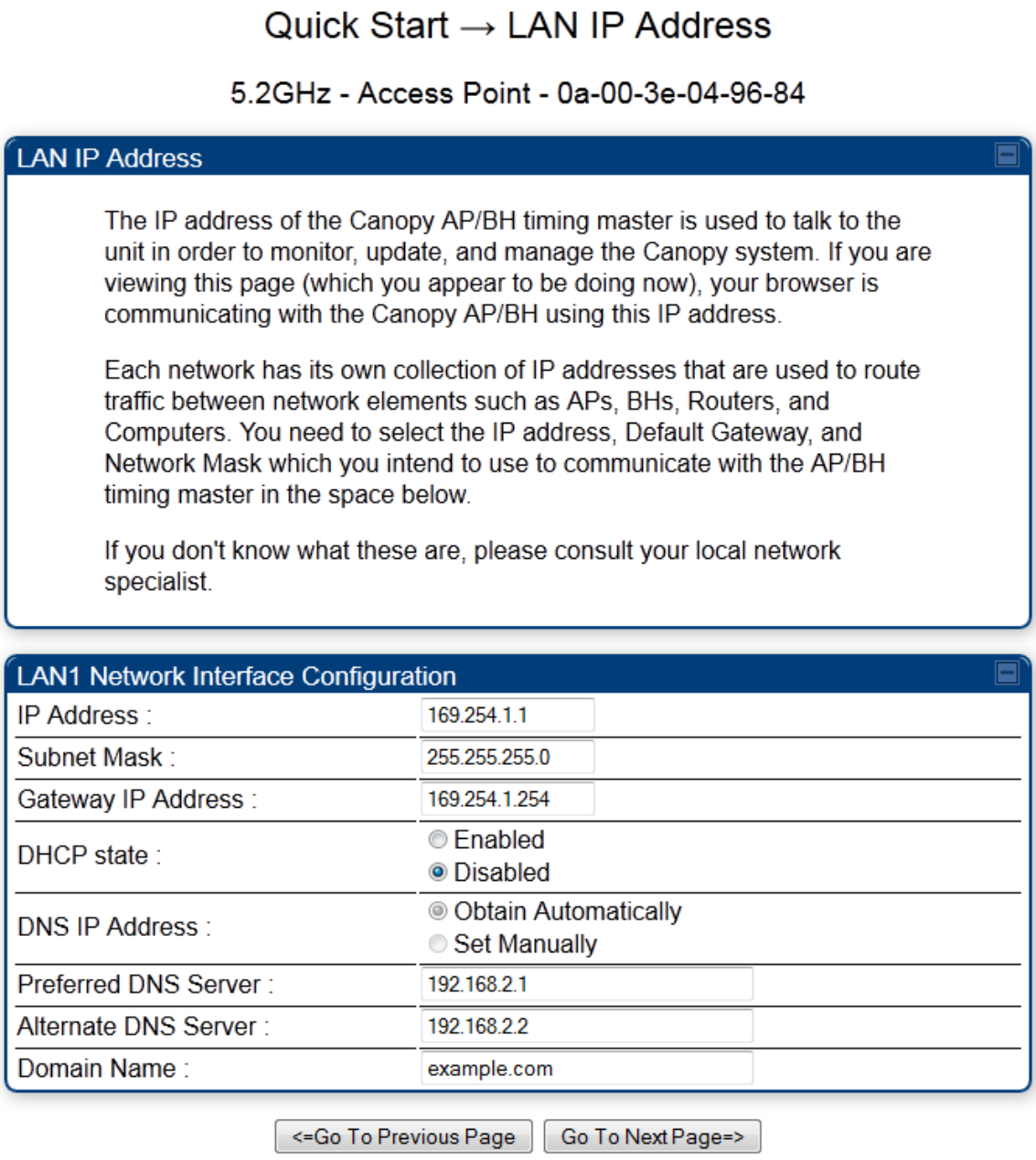

Quick Start → LAN IP Address
5.2GHz - Access Point - 0a-00-3e-04-96-84
LAN IP Address
The IP address of the Canopy AP/BH timing master is used to talk to the unit in order to monitor, update, and manage the Canopy system. If you are viewing this page (which you appear to be doing now), your browser is communicating with the Canopy AP/BH using this IP address.
Each network has its own collection of IP addresses that are used to route traffic between network elements such as APs, BHs, Routers, and Computers. You need to select the IP address, Default Gateway, and Network Mask which you intend to use to communicate with the AP/BH timing master in the space below.
If you don't know what these are, please consult your local network specialist.
LAN1 Network Interface Configuration
IP Address : 169.254.1.1
Subnet Mask : 255.255.255.0
Gateway IP Address : 169.254.1.254
DHCP state : Enabled Disabled
DNS IP Address : Obtain Automatically Set Manually
Preferred DNS Server : 192.168.2.1
Alternate DNS Server : 192.168.2.2
Domain Name : example.com
<=Go To Previous Page
Go To Next Page=>

Figure 64: LAN IP Address tab of AP, example

8. At the bottom of this tab, either
   - specify an **IP Address**, a **Subnet Mask**, and a **Gateway IP Address** for management of the AP and leave the **DHCP state** set to **Disabled**.
   - set the **DHCP state** to **Enabled** to have the IP address, subnet mask, and gateway IP address automatically configured by a domain name server (DNS).

NOTE:
Cambium encourages you to experiment with the interface. Unless you save a configuration and reboot the AP after you save the configuration, none of the changes are effected.

9. Click the **Go To Next Page =>** button.
   RESULT: The AP responds by opening the Review and Save Configuration tab. An example of this tab is shown in Figure 65.

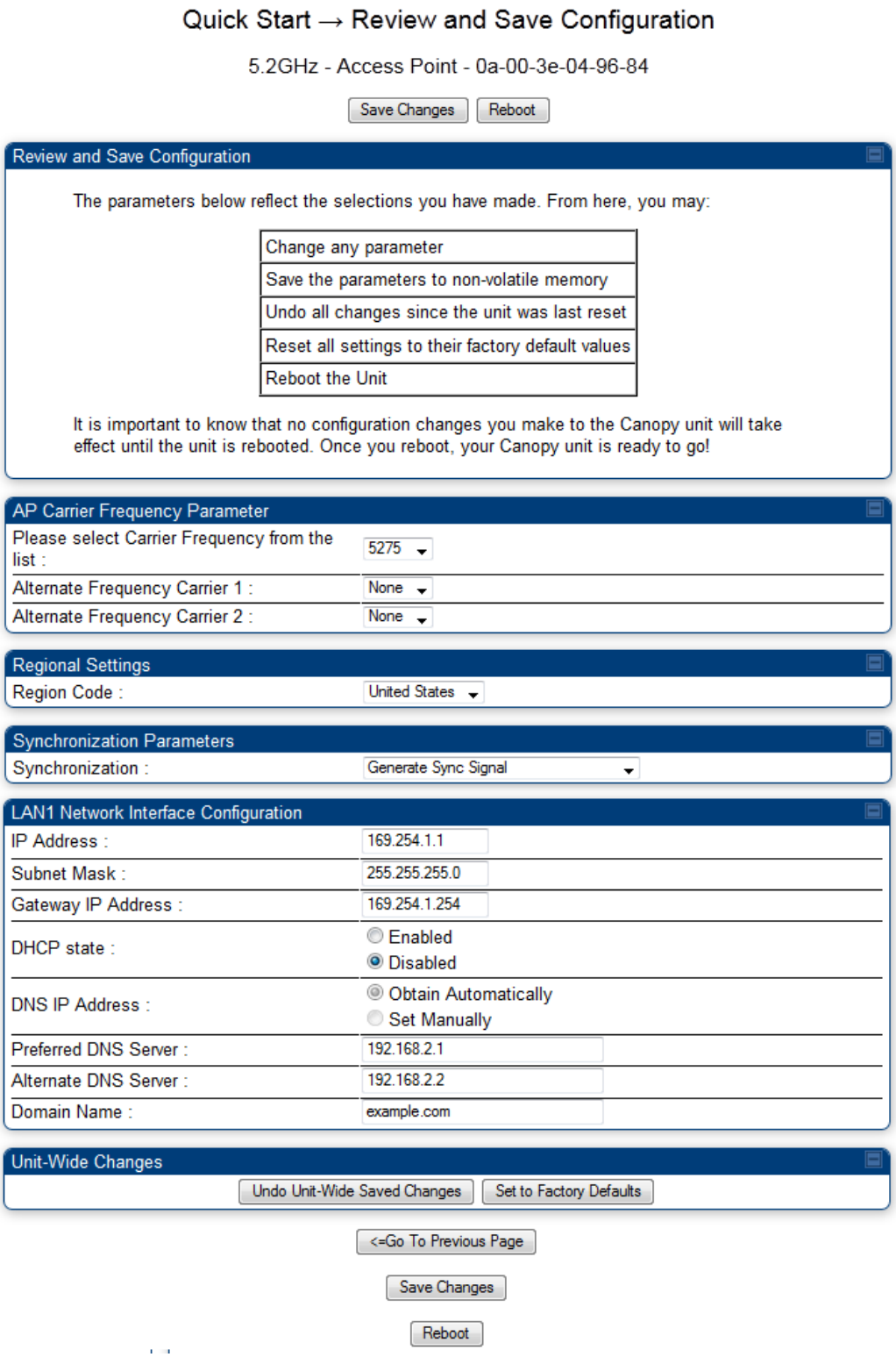


Figure 65: Review and Save Configuration tab of AP, example

10. Ensure that the initial parameters for the AP are set as you intended.
11. Click the **Save Changes** button.
12. Click the **Reboot** button.
    RESULT: The AP responds with the message **Reboot Has Been Initiated…**
13. Wait until the indicator LEDs are not red.
14. Trigger your browser to refresh the page until the AP redisplays the General Status tab.
15. Wait until the red indicator LEDs are not lit.

Time Tab of the AP

To proceed with the test setup, click the **Configuration** link on the left side of the General Status tab. When the AP responds by opening the Configuration page to the General tab, click the Time tab. An example of this tab is displayed in Figure 66.

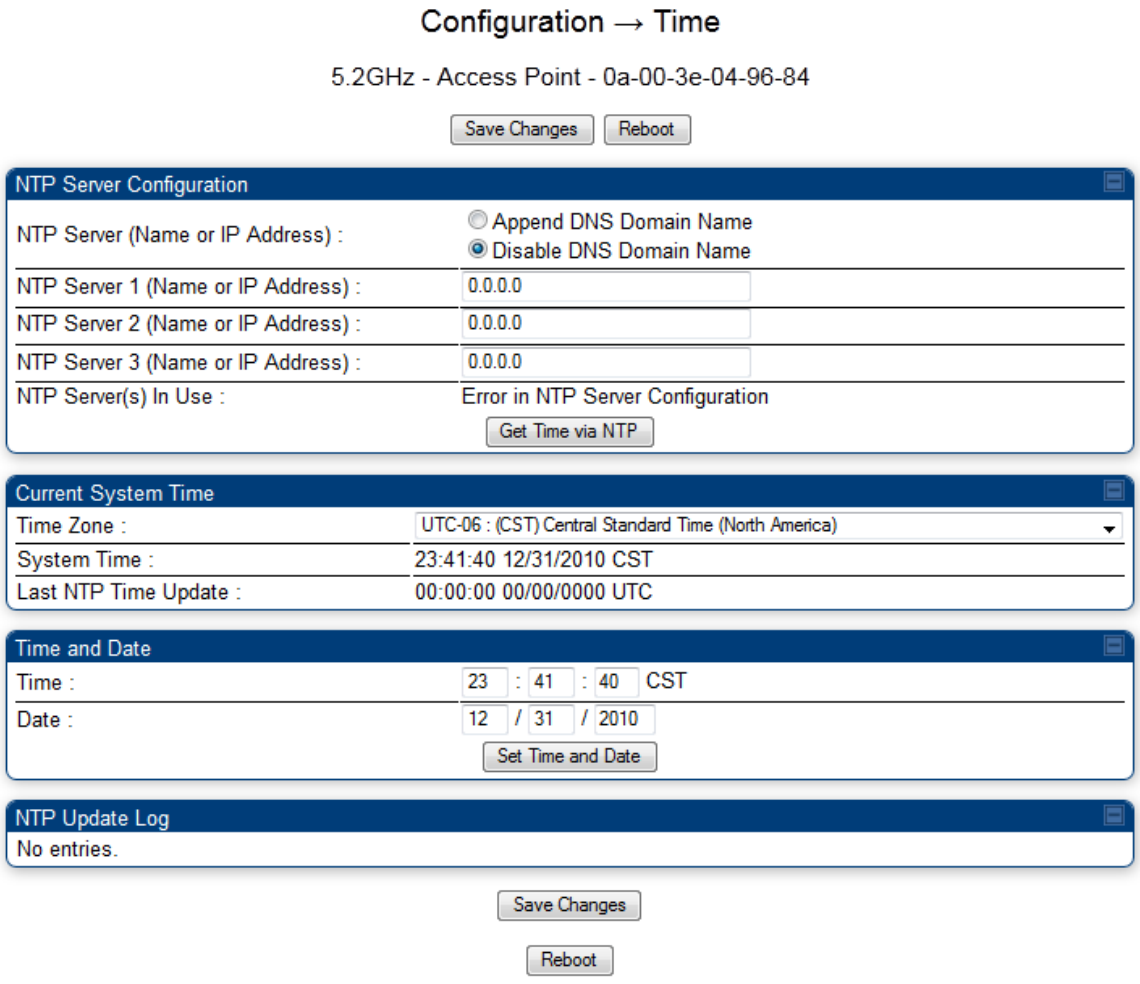


Figure 66: Time tab of AP, example

To have each log in the AP correlated to a meaningful time and date, either a reliable network element must pass time and date to the AP or you must set the time and date whenever a power cycle of the AP has occurred. A network element passes time and date in any of the following scenarios:

- A connected CMM2 passes time and date (GPS time and date, if received).
- A connected CMMmicro passes the time and date (GPS time and date, if received), but only if both the CMMmicro is operating on CMMmicro Release 2.1 or later release. (These releases include an NTP server functionality.)
- A separate NTP server is addressable from the AP.

If the AP should obtain time and date from a CMMmicro, CMM4, or a separate NTP server, enter the IP address of the CMM or NTP server on this tab. To force the AP to obtain time and date before the first (or next) 15-minute interval query of the NTP server, click **Get Time through NTP**.

If you enter a time and date, the format for entry is

Time : ***hh*** / ***mm*** / ***ss***

Date : ***MM*** / ***dd*** / ***yyyy***

where

hh	represents the two-digit hour in the range 00 to 24
mm	represents the two-digit minute
ss	represents the two-digit second
MM	represents the two-digit month
dd	represents the two-digit day
yyyy	represents the four-digit year

Proceed with the test setup as follows.

- Enter the appropriate information in the format shown above.
- Then click the **Set Time and Date** button.
  NOTE: The time displayed at the top of this page is static unless your browser is set to automatically refresh.

Procedure 8: Setting up the SM for test

1. In one hand, securely hold the top (larger shell) of the SM. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
2. Plug one end of a CAT 5 Ethernet cable into the SM RJ-45 jack.
3. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.
4. Roughly aim the SM toward the AP.

WARNING!
From this point until you remove power from the SM, stay at least as far from the SM as the minimum separation distance specified in Table 43 on Page 174.

5. Plug the power supply into an electrical outlet.
6. Repeat the foregoing steps for each SM that you wish to include in the test.
7. Back at the computing device, on the left side of the Time & Date tab, click **Home**.
8. Click the Session Status tab.

Session Status Tab of the AP

An example of the AP Session Status tab is displayed in Figure 67.

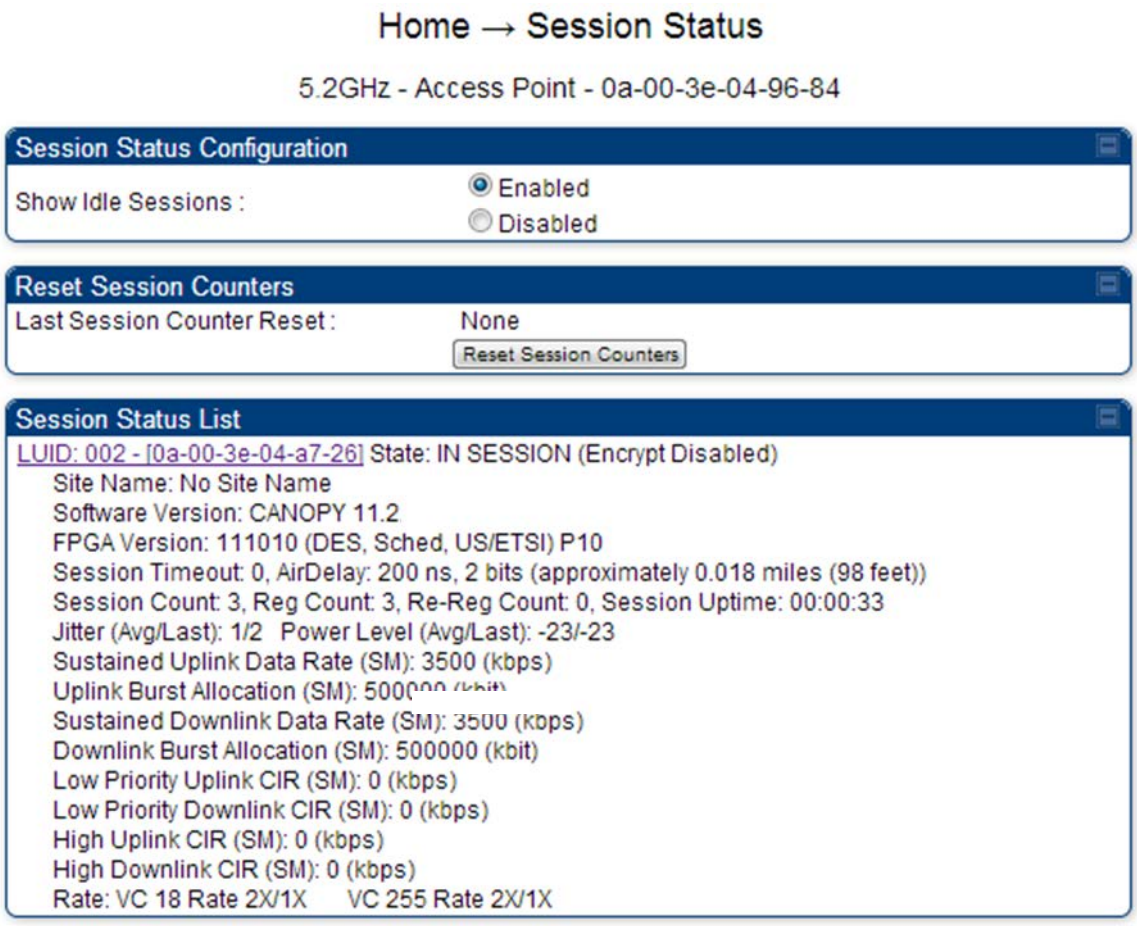

Home → Session Status
5.2GHz - Access Point - 0a-00-3e-04-96-84
Session Status Configuration
Show Idle Sessions :
Enabled
Disabled
Reset Session Counters
Last Session Counter Reset :
None
Reset Session Counters
Session Status List
LUID: 002 - [0a-00-3e-04-a7-26] State: IN SESSION (Encrypt Disabled)
Site Name: No Site Name
Software Version: CANOPY 11.2
FPGA Version: 111010 (DES, Sched, US/ETSI) P10
Session Timeout: 0, AirDelay: 200 ns, 2 bits (approximately 0.018 miles (98 feet))
Session Count: 3, Reg Count: 3, Re-Reg Count: 0, Session Uptime: 00:00:33
Jitter (Avg/Last): 1/2 Power Level (Avg/Last): -23/-23
Sustained Uplink Data Rate (SM): 3500 (kbps)
Uplink Burst Allocation (SM): 500000 (kbit)
Sustained Downlink Data Rate (SM): 3500 (kbps)
Downlink Burst Allocation (SM): 500000 (kbit)
Low Priority Uplink CIR (SM): 0 (kbps)
Low Priority Downlink CIR (SM): 0 (kbps)
High Uplink CIR (SM): 0 (kbps)
High Downlink CIR (SM): 0 (kbps)
Rate: VC 18 Rate 2X/1X VC 255 Rate 2X/1X

Figure 67: Session Status tab data from AP, example

If no SMs are registered to this AP, then the Session Status tab displays the simple message **No sessions**. In this case, try the following steps.

Procedure 9: Retrying to establish a point-to-multipoint link

1. More finely aim the SM or SMs toward the AP.
2. Recheck the Session Status tab of the AP for the presence of LUIDs.
3. If still no LUIDs are reported on the Session Status tab, click the **Configuration** button on the left side of the Home page.
   RESULT: The AP responds by opening the AP Configuration page.
4. Click the Radio tab.
5. Find the **Color Code** parameter and note the setting.
6. In the same sequence as you did for the AP directly under Configuring a Point-to-Multipoint Link for Test on Page 190, connect the SM to a computing device and to power.
7. On the left side of the SM Home page, click the **Configuration** button.
   RESULT: The Configuration page of the SM opens.
8. Click the Radio tab.

9. If the transmit frequency of the AP is not selected in the **Custom Radio Frequency Scan Selection List** parameter, select the frequency that matches.
10. If the **Color Code** parameter on this page is not identical to the **Color Code** parameter you noted from the AP, change one of them so that they match.
11. At the bottom of the Radio tab for the SM, click the **Save Changes** button.
12. Click the **Reboot** button.
13. Allow several minutes for the SM to reboot and register to the AP.
14. Return to the computing device that is connected to the AP.
15. Recheck the Session Status tab of the AP for the presence of LUIDs.

The Session Status tab provides information about each SM that has registered to the AP. This information is useful for managing and troubleshooting a system. All information that you have entered in the **Site Name** field of the SM displays in the Session Status tab of the linked AP.

The Session Status tab also includes the current active values on each SM (LUID) for MIR, CIR, and VLAN, as well as the source of these values (representing the SM itself, BAM, or the AP and cap, if any—for example, APCAP as shown in Figure 67 above). L indicates a Lite SM (CSM 110), and D indicates from the device. As an SM registers to the AP, the configuration source that this page displays for the associated LUID may change. After registration, however, the displayed source is stable and can be trusted.

The Session Status tab of the AP provides the following parameters.

Show Idle Sessions

Idle subscribers may be included or removed from the session status display by enabling or disabling, respectively, the **Show Idle Sessions** parameter. Enabling or disabling this parameter only affects the GUI display of subscribers, not the registration status.

LUID

This field displays the LUID (logical unit ID) of the SM. As each SM registers to the AP, the system assigns an LUID of 2 or a higher unique number to the SM. If an SM loses registration with the AP and then regains registration, the SM will retain the same LUID.

NOTE:
The LUID association is lost when a power cycle of the AP occurs.

Both the LUID and the MAC are hot links to open the interface to the SM. In some instances, depending on network activity and network design, this route to the interface yields a blank web page. If this occurs, refresh your browser view.

MAC

This field displays the MAC address (or electronic serial number) of the SM. Both the LUID and the MAC are hot links to open the interface to the SM. In some instances, depending on network activity and network design, this route to the interface yields a blank web page. If this occurs, refresh your browser view.

State

This field displays the current status of the SM as either

- **IN SESSION** to indicate that the SM is currently registered to the AP.
- **IDLE** to indicate that the SM was registered to the AP at one time, but now is not.

This field also indicates whether the encryption scheme in the module is enabled.

Site Name

This field indicates the name of the SM. You can assign or change this name on the Configuration web page of the SM. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Software Version

This field displays the software release that operates on the SM, the release date and time of the software.

FPGA Version

This field displays the version of FPGA that runs on the SM.

Session Timeout

This field displays the timeout in seconds for management sessions via HTTP, telnet, or ftp access to the SM. 0 indicates that no limit is imposed.

AirDelay

This field displays the distance of the SM from the AP. To derive the distance in meters, multiply the displayed number by 0.3048. At close distances, the value in this field is unreliable.

Session Count

This field displays how many sessions the SM has had with the AP. Typically, this is the sum of Reg Count and Re-Reg Count. However, the result of internal calculation may display here as a value that slightly differs from the sum.

If the number of sessions is significantly greater than the number for other SMs, then this may indicate a link problem or an interference problem.

Reg Count

When an SM makes a registration request, the AP checks its local data to see whether it considers the SM to be already registered. If the AP concludes that the SM is not, then the request increments the value of this field.

Re-Reg Count

When an SM makes a registration request, the AP checks its local data to see whether it considers the SM to be already registered. If the AP concludes that the SM is not, then the request increments the value of this field. Typically, a Re-Reg is the case where both

- an SM attempts to reregister for having lost communication with the AP.
- the AP has not yet observed the link to the SM as being down.

A high number in this field is often an indication of link instability or interference problems.

RSSI, Jitter, and Power Level (Avg/Last)

The Session Status tab shows the received **Power Level** in dBm and **Jitter**. Proper alignment maximizes **Power Level** and minimizes **Jitter**. As you refine alignment, you should favor lower jitter over higher dBm.

For example, if coarse alignment gives an SM a power level of −75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to −78 dBm and the jitter to 2 or 3, use the refined alignment, with the following caveats:

- When the receiving link is operating at 1X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 4.
- When the receiving link is operating at 2X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 9.

However, Jitter is not calculated and reported in the PMP 400 Series OFDM AP. The Session Status tab also shows a historical **RSSI**, a unitless measure of power. Use **Power Level** and ignore **RSSI**. **RSSI** implies more accuracy and precision than is inherent in its measurement.

In both an FSK and an OFDM module, the spectrum analyzer measures and displays the detected *peak* power level. This is consistent with the received Power Level that various tabs in the FSK modules report. However, it is inconsistent with received Power Level indications in OFDM modules, which use this parameter to report the detected *average* power level. For this reason, you will observe a difference in how the spectrum analyzer and the Power Level field separately report on the same OFDM signal at the same time.

Sustained Uplink Data Rate

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified rate at which each SM registered to this AP is replenished with credits for transmission. The configuration source of the value is indicated in parentheses. See

- Maximum Information Rate (MIR) Parameters on Page 83
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 86
- Setting the Configuration Source on Page 324.

Uplink Burst Allocation

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified maximum amount of data that each SM is allowed to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more. The configuration source of the value is indicated in parentheses. See

- Maximum Information Rate (MIR) Parameters on Page 83
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 86
- Setting the Configuration Source on Page 324.

Sustained Downlink Data Rate

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified the rate at which the AP should be replenished with credits (tokens) for transmission to each of the SMs in its sector. The configuration source of the value is indicated in parentheses. See

- Maximum Information Rate (MIR) Parameters on Page 83
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 86
- Setting the Configuration Source on Page 324.

Downlink Burst Allocation

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the maximum amount of data to allow the AP to transmit to any registered SM before the AP is replenished with transmission credits at the **Sustained Downlink Data Rate**. The configuration source of the value is indicated in parentheses. See

- Maximum Information Rate (MIR) Parameters on Page 83
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 86
- Setting the Configuration Source on Page 324.

Low Priority Uplink CIR

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. The configuration source of the value is indicated in parentheses. See

- Committed Information Rate on Page 85
- Setting the Configuration Source on Page 324.

Low Priority Downlink CIR

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. The configuration source of the value is indicated in parentheses. See

- Committed Information Rate on Page 85
- Setting the Configuration Source on Page 324.

Rate

This field displays whether the high-priority channel is enabled in the SM and the status of 1X or 2X operation in the SM. See Checking the Status of 2X Operation on Page 91.

Beginning the Test of Point-to-Multipoint Links

To begin the test of links, perform the following steps:

1. In the Session Status tab of the AP, note the LUID associated with the MAC address of any SM you wish to involve in the test.
2. Click the Remote Subscribers tab.

Remote Subscribers Tab of the AP

An example of a Remote Subscribers tab is displayed in Figure 68.

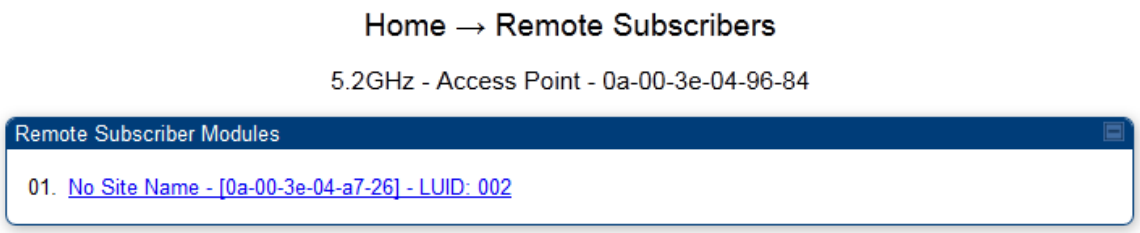

Home → Remote Subscribers
5.2GHz - Access Point - 0a-00-3e-04-96-84
Remote Subscriber Modules
01. No Site Name - [0a-00-3e-04-a7-26] - LUID: 002

Figure 68: Remote Subscribers tab of AP, example

This tab allows you to view the web pages of registered SMs over the RF link. To view the pages for a selected SM, click its link. The General Status tab of the SM opens.

General Status Tab of the SM

An example of the General Status tab of an SM is displayed in Figure 69.

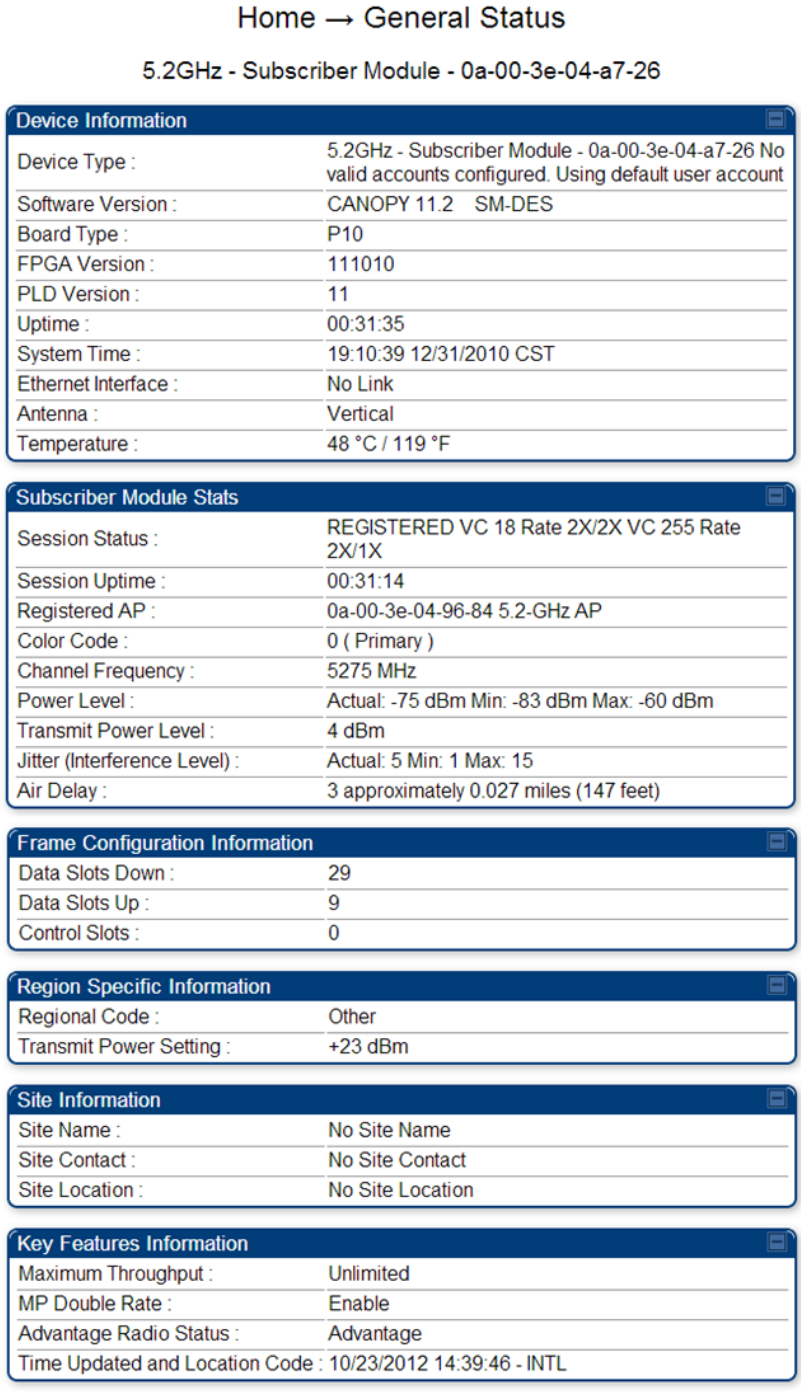

Home → General Status
5.2GHz - Subscriber Module - 0a-00-3e-04-a7-26
Device Information
Device Type : 5.2GHz - Subscriber Module - 0a-00-3e-04-a7-26 No valid accounts configured. Using default user account
Software Version : CANOPY 11.2 SM-DES
Board Type : P10
FPGA Version : 111010
PLD Version : 11
Uptime : 00:31:35
System Time : 19:10:39 12/31/2010 CST
Ethernet Interface : No Link
Antenna : Vertical
Temperature : 48 °C / 119 °F
Subscriber Module Stats
Session Status : REGISTERED VC 18 Rate 2X/2X VC 255 Rate 2X/1X
Session Uptime : 00:31:14
Registered AP : 0a-00-3e-04-96-84 5.2-GHz AP
Color Code : 0 (Primary)
Channel Frequency : 5275 MHz
Power Level : Actual: -75 dBm Min: -83 dBm Max: -60 dBm
Transmit Power Level : 4 dBm
Jitter (Interference Level) : Actual: 5 Min: 1 Max: 15
Air Delay : 3 approximately 0.027 miles (147 feet)
Frame Configuration Information
Data Slots Down : 29
Data Slots Up : 9
Control Slots : 0
Region Specific Information
Regional Code : Other
Transmit Power Setting : +23 dBm
Site Information
Site Name : No Site Name
Site Contact : No Site Contact
Site Location : No Site Location
Key Features Information
Maximum Throughput : Unlimited
MP Double Rate : Enable
Advantage Radio Status : Advantage
Time Updated and Location Code : 10/23/2012 14:39:46 - INTL

Figure 69: General Status tab of SM, example

The General Status tab provides information on the operation of this SM. This is the tab that opens by default when you access the GUI of the SM. The General Status tab provides the following read-only fields.

Device Type

This field indicates the type of the module. Values include the frequency band of the SM, its module type, and its MAC address.

Software Version

This field indicates the system release, the time and date of the release, and whether communications involving the module are secured by DES or AES encryption (see Encrypting Radio Transmissions on Page 428). If you request technical support, provide the information from this field.

Board Type

This field indicates the series of hardware. See Designations for Hardware in Radios on Page 425.

FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.

PLD Version

This field indicates the version of the programmable logic device (PLD) on the module. If you request technical support, provide the value of this field.

Uptime

This field indicates how long the module has operated since power was applied.

System Time

This field provides the current time. Any SM that registers to an AP inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).

Ethernet Interface

This field indicates the speed and duplex state of the Ethernet interface to the SM.

Antenna

The presence of this field depends on whether antenna options are available for the module. This field indicates the polarity of the antenna in the modules as one of the following:

- Horizontal
- Vertical
- External (Connectorized)

Temperature

This field displays the current operating temperature of the device (range −40°C to +55°C (−40°F to 131°F)).

Session Status

This field displays the following information about the current session:

- **Scanning** indicates that this SM currently cycles through the radio frequencies that are selected in the Radio tab of the Configuration page.
- **Syncing** indicates that this SM currently attempts to receive sync.
- **Registering** indicates that this SM has sent a registration request message to the AP and has not yet received a response.
- **Registered** indicates that this SM is both
  - registered to an AP.
  - ready to transmit and receive data packets.
- **Alignment** indicates that this SM is in an aiming mode. See Table 47 on Page 186.

Session Uptime

This field displays the duration of the current link. The syntax of the displayed time is *hh:mm:ss*.

Registered AP

This field displays the MAC address of the AP to which this SM is registered.

Power Level and Jitter

The General Status tab shows the received **Power Level** in dBm and **Jitter**. Proper alignment maximizes **Power Level** and minimizes **Jitter**. As you refine alignment, you should favor lower jitter over higher dBm. For example, if coarse alignment gives an SM a power level of −75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to −78 dBm and the jitter to 2 or 3, use the refined alignment, with the following caveats:

- When the receiving link is operating at 1X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 4.
- When the receiving link is operating at 2X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 9.

PMP 400 Series OFDM SMs do not have this parameter. For historical relevance, the General Status tab also shows the **RSSI**, the unitless measure of power. Use **Power Level** and ignore **RSSI**. **RSSI** implies more accuracy and precision than is inherent in its measurement.

NOTE:
Unless the page is set to auto-refresh, the values displayed are from the instant the General Status tab was selected. To keep a current view of the values, refresh the browser screen or set to auto-refresh.

Air Delay

This field displays the distance in feet between this SM and the AP. To derive the distance in meters, multiply the value of this parameter by 0.3048. Distances reported as less than 200 feet (61 meters) are unreliable.

Data Slots Down

This field indicates the number of frame slots that are designated for use by data traffic in the downlink (sent from the AP to the SM). The AP calculates the number of data slots based on the **Max Range**, **Downlink Data**, and (reserved) **Control Slots** configured by the operator. See Max Range on Page 249 and Downlink Data on Page 250.

A + in this field (for example, 28+) indicates that there are additional bit times that the scheduler can take advantage of for internal system communication, but not enough for a full data slot.

Data Slots Up

This field indicates the number of frame slots that are designated for use by data traffic in the uplink (sent from the SM to the AP). The AP calculates the number of data slots based on the Max Range, Downlink Data, and (reserved) Control Slots configured by the operator. See Max Range on Page 249 and Downlink Data on Page 250.

A + in this field (for example, 9+) indicates that there are additional bit times that the scheduler can take advantage of for control slots (which are half the size of data slots), but not enough for a full data slot.

Control Slots

This field indicates the number of (reserved) control slots configured by the operator. Control slots are half the size of data slots. The SM uses reserved control slots and unused data slots for bandwidth requests. See Control Slots on Page 250.

Region Code

From the drop-down list, select the region in which the radio is operating.

When the appropriate region is selected in this parameter, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard. For further information on DFS, see Radar Signature Detection and Shutdown on Page 127.

The slave radio automatically inherits the DFS type of the master. This behavior ignores the value of the **Region Code** parameter in the slave, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), you should always set the value that corresponds to the local region.

Unlike selections in other parameters, your **Region Code** selection requires a **Save Changes** and a **Reboot** cycle before it will force the context-sensitive GUI to display related options (for example, **Alternate Frequency Carrier *1 and 2*** in the Configuration => Radio tab). Thus, a proper configuration exercise in environments that are subject to DFS requirements has two imperative **Save Changes** and **Reboot** cycles: one after the **Region Code** is set, and a second after related options are set.

Site Name

This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the SM Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Contact

This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the SM Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Location

This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the SM Configuration page.

Maximum Throughput

This field indicates the limit of aggregate throughput for the SM and is based on the default (factory) limit of the SM and any floating license that is currently assigned to it.

MP Double Rate

This field indicates whether 2X modulation rate is enabled for the sector.

Advantage Radio Status

This field reflects whether the SM is currently licensed for enhanced caps (Advantage, also known as Cap 2) on uplink and downlink traffic.

Time Updated and Location Code

This field displays information about the keying of the radio.

Continuing the Test of Point-to-Multipoint Links

To resume the test of links, perform the following steps.

Procedure 10: Verifying and recording information from SMs

1. Verify that the **Session Status** field of the General Status tab in the SM indicates **REGISTERED**.
2. While you view the General Status tab in the SM, note (or print) the values of the following fields:
   - **Device type**
   - **Software Version**
   - **Board Type**
   - **FPGA Version**
3. Systematically ensure that you can retrieve this data (from a database, for example) when you later prepare to deploy the SM to subscriber premises.
4. Return to the Remote Subscribers tab of the AP.
5. Click the link of the next SM that you wish to test.
6. Repeat the test procedure from that point. When you have tested all of the SMs that you intend to test, return your browser to the General Status tab of the AP.

General Status Tab of the AP

An example of the AP General Status tab is displayed in Figure 70.

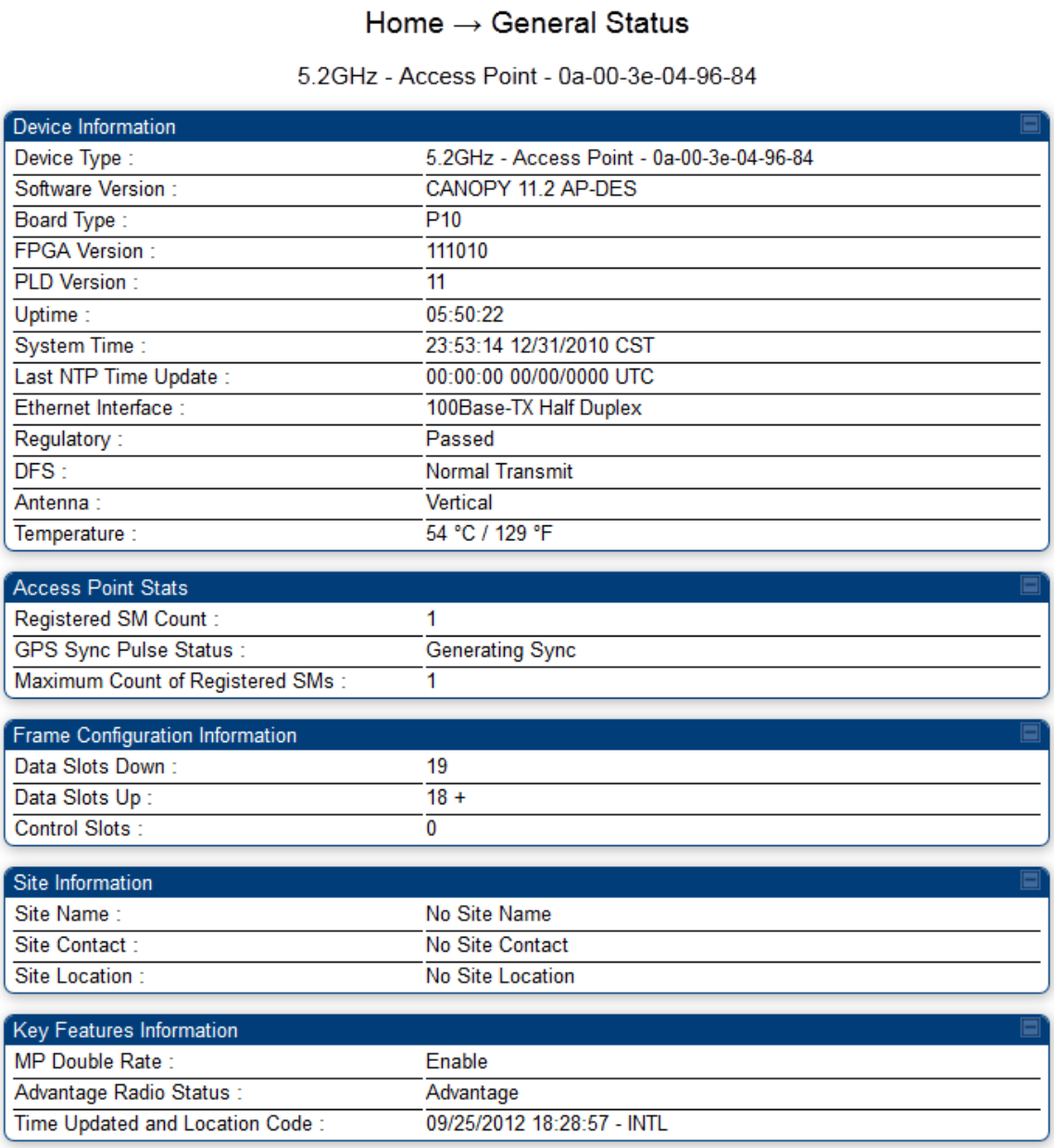

Home → General Status
5.2GHz - Access Point - 0a-00-3e-04-96-84
Device Information
Device Type : 5.2GHz - Access Point - 0a-00-3e-04-96-84
Software Version : CANOPY 11.2 AP-DES
Board Type : P10
FPGA Version : 111010
PLD Version : 11
Uptime : 05:50:22
System Time : 23:53:14 12/31/2010 CST
Last NTP Time Update : 00:00:00 00/00/0000 UTC
Ethernet Interface : 100Base-TX Half Duplex
Regulatory : Passed
DFS : Normal Transmit
Antenna : Vertical
Temperature : 54 °C / 129 °F
Access Point Stats
Registered SM Count : 1
GPS Sync Pulse Status : Generating Sync
Maximum Count of Registered SMs : 1
Frame Configuration Information
Data Slots Down : 19
Data Slots Up : 18 +
Control Slots : 0
Site Information
Site Name : No Site Name
Site Contact : No Site Contact
Site Location : No Site Location
Key Features Information
MP Double Rate : Enable
Advantage Radio Status : Advantage
Time Updated and Location Code : 09/25/2012 18:28:57 - INTL

Figure 70: General Status tab of AP, example

The General Status tab provides information on the operation of this AP. This is the tab that opens by default when you access the GUI of the AP. The General Status tab provides the following read-only fields.

Device Type

This field indicates the type of the module. Values include the frequency band of the AP, its module type, and its MAC address.

Software Version

This field indicates the system release, the time and date of the release, and whether communications involving the module are secured by DES or AES encryption (see Encrypting Radio Transmissions on Page 428). If you request technical support, provide the information from this field.

Board Type

This field indicates the series of hardware. See Designations for Hardware in Radios on Page 425.

FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. If you request technical support, provide the value of this field.

PLD Version

This field indicates the version of the programmable logic device (PLD) on the module. If you request technical support, provide the value of this field.

Uptime

This field indicates how long the module has operated since power was applied.

System Time

This field provides the current time. If the AP is connected to a CMM, then this field provides GMT (Greenwich Mean Time). Any SM that registers to the AP inherits the system time.

Last NTP Time Update

This field displays when the AP last used time sent from an NTP server. If the AP has not been configured in the Time tab of the Configuration page to request time from an NTP server, then this field is populated by 00:00:00 00/00/00.

Ethernet Interface

This field indicates the speed and duplex state of the Ethernet interface to the AP.

Regulatory

This field indicates whether the configured Region Code and radio frequency are compliant with respect to their compatibility. For example, you may configure a 5.4-GHz AP with a **Region Code** set to **United States** and configure a frequency that lies within the weather notch. This is a compliant combination, the radio properly operates, and its **Regulatory** field displays Passed. If later you change its Region Code to Canada, then the combination becomes non-compliant (since frequencies within the weather notch are disallowed in Canada. In this case, the radio ceases to transmit, and its **Regulatory** field displays an error message.

For further information on Region Codes and DFS, see Radar Signature Detection and Shutdown on Page 127.

Antenna

The presence of this field depends on whether antenna options are available for the module. This field indicates the polarity of the antenna in the modules as one of the following:

- Horizontal
- Vertical
- External (Connectorized)

Temperature

This field displays the current operating temperature of the device (range −40°C to +55°C (−40°F to 131°F)).

Registered SM Count

This field indicates how many SMs are registered to the AP.

GPS Sync Pulse Status

This field indicates the status of synchronization as follows:

- **Generating sync** indicates that the module is set to *generate* the sync pulse.
- **Receiving Sync** indicates that the module is set to *receive* a sync pulse from an outside source and is receiving the pulse.
- **ERROR: No Sync Pulse** indicates that the module is set to *receive* a sync pulse from an outside source and is not receiving the pulse.

NOTE:
When this message is displayed, the AP transmitter is turned off to avoid self-interference within the system.

Max Registered SM Count

This field displays the largest number of SMs that have been simultaneously registered in the AP since it was last rebooted. This count can provide some insight into sector history and provide comparison between current and maximum SM counts at a glance.

Data Slots Down

This field indicates the number of frame slots that are designated for use by data traffic in the downlink (sent from the AP to the SM). The AP calculates the number of data slots based on the **Max Range**, **Downlink Data**, and (reserved) **Control Slots** configured by the operator. See Max Range on Page 249 and Downlink Data on Page 250.

A + in this field (for example, 28+) indicates that there are additional bit times that the scheduler can take advantage of for internal system communication, but not enough for a full data slot.

Data Slots Up

This field indicates the number of frame slots that are designated for use by data traffic in the uplink (sent from the SM to the AP). The AP calculates the number of data slots based on the Max Range, Downlink Data, and (reserved) Control Slots configured by the operator. See Max Range on Page 249 and Downlink Data on Page 250.

A + in this field (for example, 9+) indicates that there are additional bit times that the scheduler can take advantage of for control slots (which are half the size of data slots), but not enough for a full data slot.

Control Slots

This field indicates the number of (reserved) control slots configured by the operator. Control slots are half the size of data slots. The SM uses reserved control slots and unused data slots for bandwidth requests. See Control Slots on Page 250.

Site Name

This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the AP Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Contact

This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Location

This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page.

MP Double Rate

This field indicates whether 2X modulation rate is enabled for the sector.

Scheduling Type

This field indicates the type of frame scheduler that is active in the AP.

Advantage Radio Status

This field indicates whether the radio is operating as an Advantage or a standard radio.

Time Updated and Location Code

This field displays information about the keying of the radio.

Concluding the Test of Point-to-Multipoint Links

To conclude the test, perform the following steps.

Procedure 11: Verifying and recording information from the AP

1. Confirm that the **GPS Sync Pulse Status** field indicates **Generating Sync**.
   NOTE: This indication confirms that the AP is properly functional.
2. While your browser is directed to this General Status tab, note (or print) the values of the following fields:
   - **Device type**
   - **Software Version**
   - **Board Type**
   - **FPGA Version**
3. Systematically ensure that you can retrieve this data when you prepare to deploy the AP.

Configuring a Point-to-Point Link for Test

Perform the following steps to begin the test setup.

Procedure 12: Setting up the BH for Quick Start

1. In one hand, securely hold the top (larger shell) of the BH that you intend to deploy as a timing master. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
2. Plug one end of a CAT 5 Ethernet cable into the timing master.
3. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.
4. Plug the other connector of the pig tail into the Ethernet jack of the computing device.

WARNING!
From this point until you remove power from the BH, stay at least as far from the BH as the minimum separation distance specified in Table 43 on Page 174.

5. Plug the power supply into an electrical outlet.
6. Power up the computing device.
7. Start the browser in the computing device.

The PTP 100 Series BH interface provides a series of web pages to configure and monitor the unit. These screens are subject to change by subsequent software releases.

You can access the web-based interface through only a computing device that is either directly connected or connected through a network to the BH. If the computing device is not connected to a network when you are configuring the module in your test environment, and if the computer has used a proxy server address and port to configure the module, then you may need to first disable the proxy setting in the computer.

To toggle the computer to *not* use the proxy setting, perform Procedure 6 on Page 190.

In the address bar of your browser, enter the IP address of the BHM (default is 169.254.1.1). The BHM responds by opening the General Status tab of its Home page.

Quick Start Page of the BHM

To proceed with the test setup, click the **Quick Start** button on the left side of the General Status tab. The BHM responds by opening the Quick Start tab of the Quick Start page. An example of this tab is displayed in Figure 71.

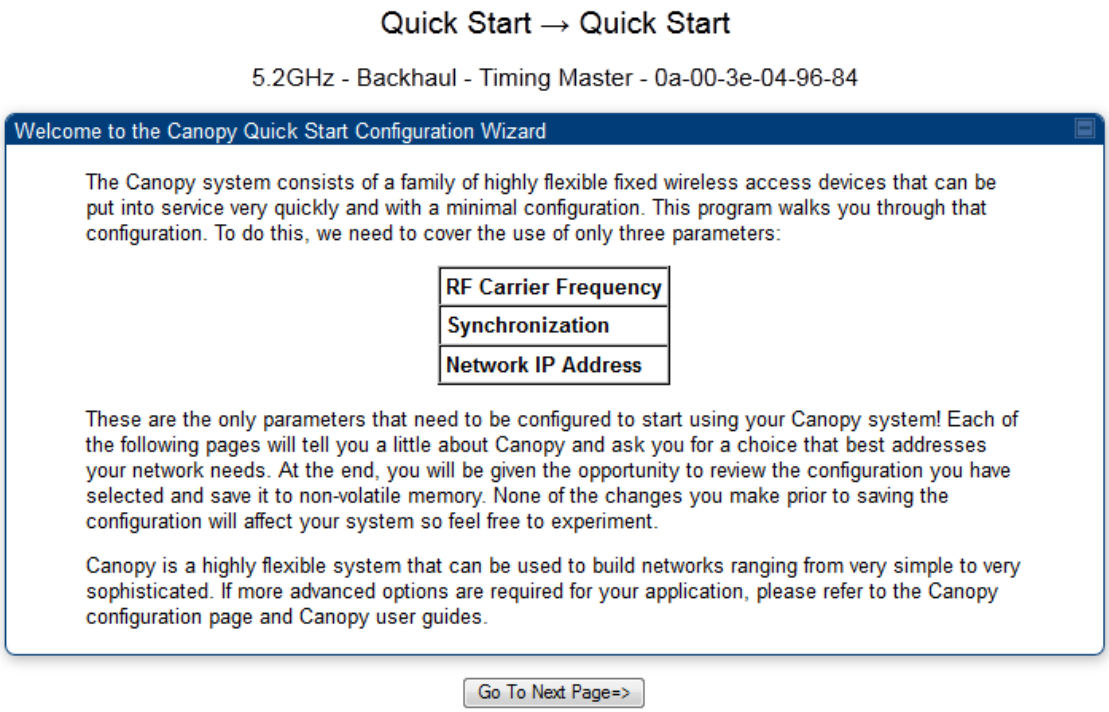

Quick Start → Quick Start
5.2GHz - Backhaul - Timing Master - 0a-00-3e-04-96-84
Welcome to the Canopy Quick Start Configuration Wizard
The Canopy system consists of a family of highly flexible fixed wireless access devices that can be put into service very quickly and with a minimal configuration. This program walks you through that configuration. To do this, we need to cover the use of only three parameters:
RF Carrier Frequency
Synchronization
Network IP Address
These are the only parameters that need to be configured to start using your Canopy system! Each of the following pages will tell you a little about Canopy and ask you for a choice that best addresses your network needs. At the end, you will be given the opportunity to review the configuration you have selected and save it to non-volatile memory. None of the changes you make prior to saving the configuration will affect your system so feel free to experiment.
Canopy is a highly flexible system that can be used to build networks ranging from very simple to very sophisticated. If more advanced options are required for your application, please refer to the Canopy configuration page and Canopy user guides.
Go To Next Page=>

Figure 71: Quick Start tab of BHM, example

Quick Start is a wizard that helps you to perform a basic configuration that places a BHM into service. Only the following variables must be configured:

- **Region Code**
- **RF Carrier Frequency**

- **Synchronization**
- **LAN (Network) IP Address**

In each page under Quick Start, you can

- specify the settings to satisfy the requirements of the network.
- review the configuration selected.
- save the configuration to non-volatile memory.

Proceed with the test setup as follows.

Procedure 13: Using Quick Start to configure the BHs for test

1. At the bottom of the Quick Start tab, click the **Go To Next Page =>** button.
   RESULT: The BHM responds by opening the Region Settings tab.
2. From the pull-down menu, select the region in which the BHM will operate.
3. Click the **Go To Next Page =>** button.
   RESULT: The BHM responds by opening the RF Carrier Frequency tab.
4. From the pull-down menu, select a frequency for the test.
5. Click the **Go To Next Page =>** button.
   RESULT: The BHM responds by opening the Synchronization tab.
6. At the bottom of this page, select **Generate Sync Signal**.
7. Click the **Go To Next Page =>** button.
   RESULT: The BHM responds by opening the LAN IP Address tab.
8. At the bottom of this tab, either
   - specify an **IP Address**, **Subnet Mask**, and **Gateway IP Address** for management of the BHM and leave the **DHCP State** set to **Disabled**.
   - set the **DHCP State** to **Enabled** to have the IP address, subnet mask, and gateway IP address automatically configured by a domain name server (DNS).
9. Click the **Go To Next Page =>** button.
   RESULT: The BHM responds by opening the Review and Save Configuration tab.
10. Ensure that the initial parameters for the BHM are set as you intended.

NOTE:
Cambium encourages you to experiment with the interface. Unless you save a configuration and reboot the BHM after you save the configuration, none of the changes are effected.

11. Click the **Save Changes** button.
12. On the left side of the tab, click the **Configuration** button.
    RESULT: The BH responds by opening the General tab of its Configuration page.
13. In the **Timing Mode** parameter, select **Timing Master**.

14. Click the **Save Changes** button.
15. Click the **Reboot** button.
    RESULT: The BHM responds with the message **Reboot Has Been Initiated…**. This BH is now forced to provide sync for the link and has a distinct set of web interface pages, tabs, and parameters for the role of BHM.
16. Wait until the indicator LEDs are not red.
17. Trigger your browser to refresh the page until the BHM redisplays the General Status tab of its Home page.
18. Repeat these steps to configure the other BH in the pair to be a BHS, selecting **Timing Slave** in Step 13.

Time Tab of the BHM

To proceed with the test setup, in the BHM, click the **Configuration** button on the left side of the General Status tab. The BHM responds by opening its Configuration page to the General tab. Click the Time tab. An example of this tab is displayed in Figure 72.

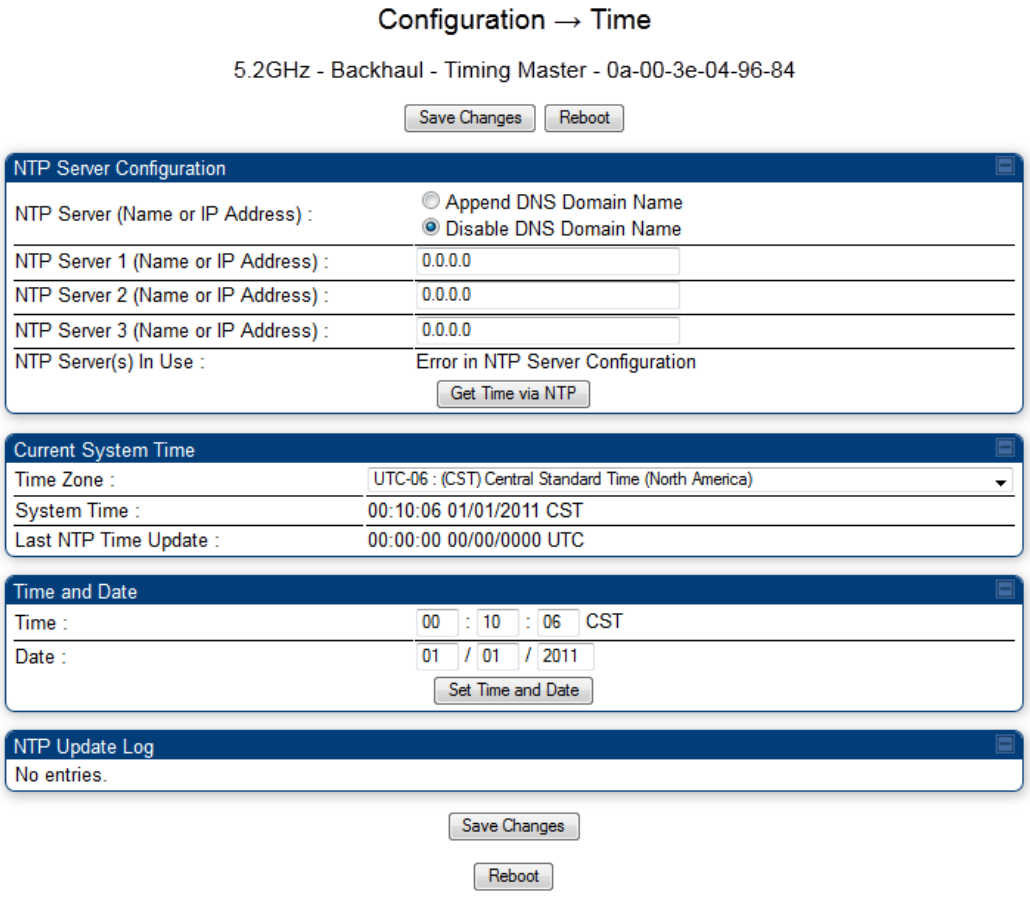


Figure 72: Time tab of BHM, example

To have each log in the BHM correlated to a meaningful time and date, either a reliable network element must pass time and date to the BHM or you must set the time and date whenever a power cycle of the BHM has occurred. A network element passes time and date in any of the following scenarios:

- A connected CMM2 passes time and date (GPS time and date, if received).
- A connected CMMmicro passes the time and date (GPS time and date, if received), but only if the CMMmicro is operating on CMMmicro Release 2.1 or later release. (These releases include an NTP server functionality.)
- A separate NTP server is addressable from the BHM.

If the BHM should derive time and date from either a CMMmicro or a separate NTP server, enter the IP address of the CMMmicro or NTP server on this tab. To force the BHM to derive time and date before the first (or next) 15-minute interval query of the NTP server, click **Get Time through NTP**.

If you enter a time and date, the format for entry is

Time : ***hh*** / ***mm*** / ***ss***

Date : ***MM*** / ***dd*** / ***yyyy***

where

hh	represents the two-digit hour in the range 00 to 24
mm	represents the two-digit minute
ss	represents the two-digit second
MM	represents the two-digit month
dd	represents the two-digit day
yyyy	represents the four-digit year

Proceed with the test setup as follows.

Procedure 14: Setting up the BHS for test

1. Enter the appropriate information in the format shown above.
2. Click the **Set Time and Date** button.
   NOTE: The time displayed at the top of this page is static unless your browser is set to automatically refresh.
3. In one hand, securely hold the top (larger shell) of the BH that you intend to deploy as a timing slave. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
4. Plug one end of a CAT 5 Ethernet cable into the BHS.
5. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.
6. Roughly aim the BHS toward the BHM.

WARNING!
From this point until you remove power from the BHS, stay at least as far from the BHS as the minimum separation distance specified in Table 43 on Page 174.

7. Plug the power supply into an electrical outlet.
8. Back at the computing device, on the left side of the BHM Time tab, click the **Home** button. When the Home page opens to the General Status tab, click the **Session Status** tab.
   RESULT: The BHM opens the Session Status tab.

Beginning the Test of Point-to-Point Links

To begin the test of your BH link, in the Remote Subscribers tab of the BHM, click the link to the BHS. The BHS GUI opens to the General Status tab of its Home page.

An example of the BHS General Status tab is displayed in Figure 73.

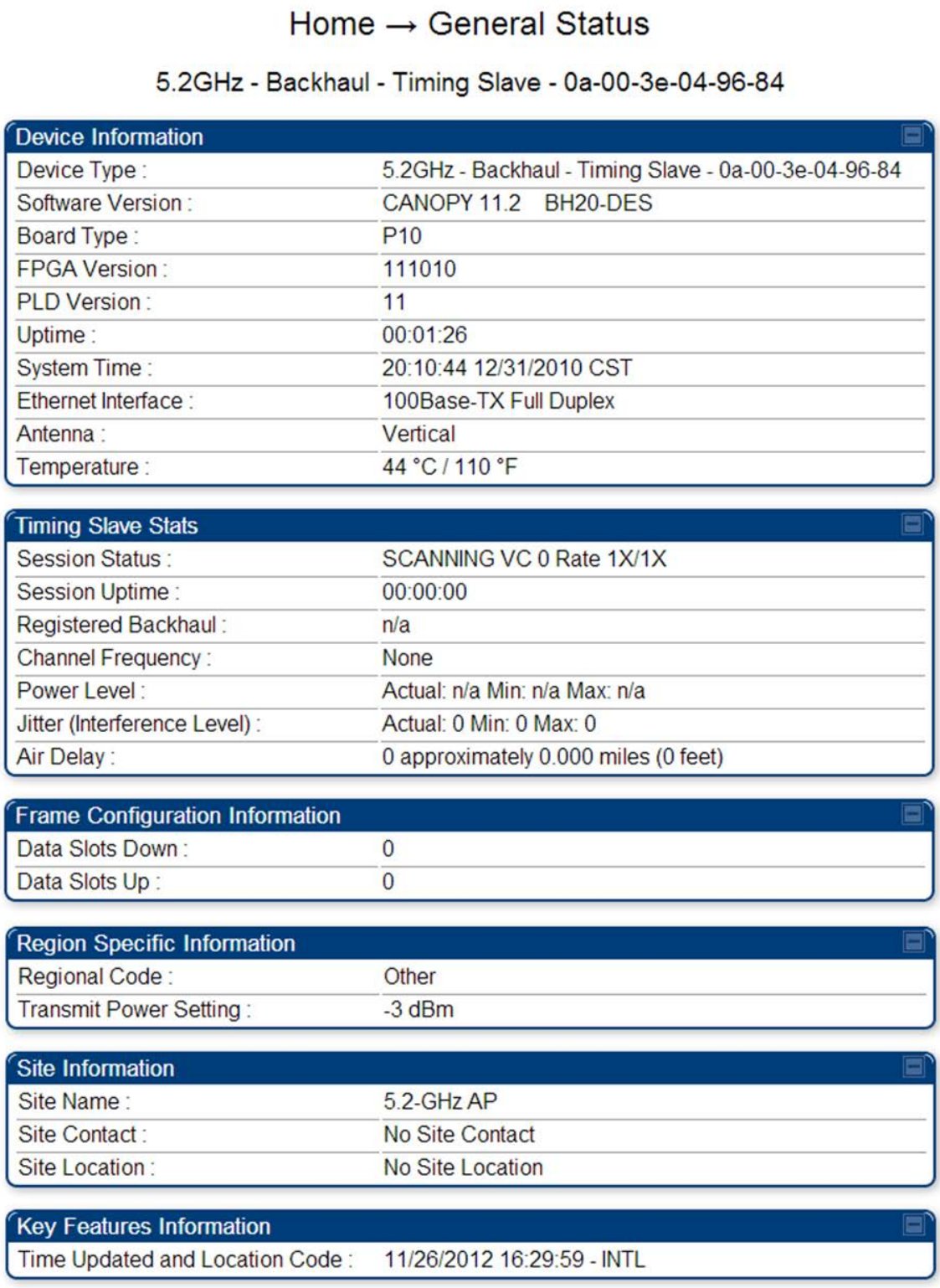

Home → General Status
5.2GHz - Backhaul - Timing Slave - 0a-00-3e-04-96-84
Device Information
Device Type : 5.2GHz - Backhaul - Timing Slave - 0a-00-3e-04-96-84
Software Version : CANOPY 11.2 BH20-DES
Board Type : P10
FPGA Version : 111010
PLD Version : 11
Uptime : 00:01:26
System Time : 20:10:44 12/31/2010 CST
Ethernet Interface : 100Base-TX Full Duplex
Antenna : Vertical
Temperature : 44 °C / 110 °F
Timing Slave Stats
Session Status : SCANNING VC 0 Rate 1X/1X
Session Uptime : 00:00:00
Registered Backhaul : n/a
Channel Frequency : None
Power Level : Actual: n/a Min: n/a Max: n/a
Jitter (Interference Level) : Actual: 0 Min: 0 Max: 0
Air Delay : 0 approximately 0.000 miles (0 feet)
Frame Configuration Information
Data Slots Down : 0
Data Slots Up : 0
Region Specific Information
Regional Code : Other
Transmit Power Setting : -3 dBm
Site Information
Site Name : 5.2-GHz AP
Site Contact : No Site Contact
Site Location : No Site Location
Key Features Information
Time Updated and Location Code : 11/26/2012 16:29:59 - INTL

Figure 73: General Status tab of BHS, example

The General Status tab provides information on the operation of this BHS. This is the tab that opens by default when you access the GUI of the BHS. The General Status tab provides the following read-only fields.

Device Type

This field indicates the type of the module. Values include the frequency band of the BHS, its module type, and its MAC address.

Software Version

This field indicates the system release, the time and date of the release, the modulation rate, and whether communications involving the module are secured by DES or AES encryption (see Encrypting Radio Transmissions on Page 428). If you request technical support, provide the information from this field.

Board Type

This field indicates the series of hardware. See Designations for Hardware in Radios on Page 425.

FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the value of this field.

PLD Version

This field indicates the version of the programmable logic device (PLD) on the module. If you request technical support, provide the value of this field.

Uptime

This field indicates how long the module has operated since power was applied.

System Time

This field provides the current time. When a BHS registers to a BHM, it inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).

Ethernet Interface

This field indicates the speed and duplex state of the Ethernet interface to the BHS.

Antenna

The presence of this field depends on whether antenna options are available for the module. This field indicates the polarity of the antenna in the modules as one of the following:

- Horizontal
- Vertical
- External (Connectorized)

Session Status

This field displays the following information about the current session:

- **Scanning** indicates that this SM currently cycles through the RF frequencies that are selected in the Radio tab of the Configuration page.
- **Syncing** indicates that this SM currently attempts to receive sync.
- **Registering** indicates that this SM has sent a registration request message to the AP and has not yet received a response.
- **Registered** indicates that this SM is both
  - registered to an AP.
  - ready to transmit and receive data packets.
- **Alignment** indicates that this SM is in an aiming mode. See Table 47 on Page 186.

Session Uptime

This field displays the duration of the current link. The syntax of the displayed time is *hh:mm:ss*.

Registered Backhaul

This field displays the MAC address of the BHM to which this BHS is registered.

Channel Frequency

This field indicates the current operating center frequency.

Power Level and Jitter

The General Status tab shows the received **Power Level** in dBm and **Jitter**. Proper alignment maximizes **Power Level** and minimizes **Jitter**. As you refine alignment, you should favor lower jitter over higher dBm. For example, if coarse alignment gives the BHS a power level of −75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to −78 dBm and the jitter to 2 or 3, use the refined alignment, with the following caveats:

- When the receiving link is operating at 1X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 4.
- When the receiving link is operating at 2X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 9.

OFDM BHSs do not have this parameter. For historical relevance, the General Status tab also shows the **RSSI**, the unitless measure of power. Use **Power Level** and ignore **RSSI**. **RSSI** implies more accuracy and precision than is inherent in its measurement.

NOTE:
Unless the page is set to auto-refresh, the values displayed are from the instant the General Status tab was selected. To keep a current view of the values, refresh the browser screen or set to auto-refresh.

Air Delay

This field displays the distance in feet between the BHS and the BHM. To derive the distance in meters, multiply the value of this parameter by 0.3048. Distances reported as less than 200 feet (61 meters) are unreliable.

Data Slots Down

This field indicates the currently configured number of frame slots that are designated for use by data traffic in the downlink (sent from the backhaul slave to the backhaul master). See Max Range on Page 249 and Downlink Data on Page 250.

Data Slots Up

This field indicates the currently configured number of frame slots that are designated for use by data traffic in the uplink (sent from the backhaul master to the backhaul slave). See Max Range on Page 249 and Downlink Data on Page 250.

Region Code

This field indicates the region in which the radio is currently set to operate. When the appropriate region has been set, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard. For further information on DFS, see Radar Signature Detection and Shutdown on Page 127.

The slave radio automatically inherits the DFS type of the master. This behavior ignores the value of the **Region Code** parameter in the slave, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), this field should always indicate the value that corresponds to the local region.

Transmit Power Setting

This field displays the value of the Transmitter Output Power parameter in the module. See Table 60: Transmitter output power settings, example cases on Page 384.

Site Name

This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the BHS Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Contact

This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the BHS Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Location

This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the BHS Configuration page.

Time Updated and Location Code

This field displays information about the keying of the radio.

Continuing the Test of Point-to-Point Links

To resume the test, perform the following steps.

Procedure 15: Verifying and recording information from the BHS

1. Verify that the **Session Status** field of the General Status tab in the BHS indicates **REGISTERED**.
   NOTE: This indication confirms that the BHS is properly functional.

2. While your browser is set to the General Status tab, note (or print) the values of the following fields:
   - **Device type**
   - **Software Version**
   - **Board Type**
   - **FPGA Version**
3. Systematically ensure that you can retrieve this data when you prepare to deploy the BHS.
4. Return your browser to the General Status tab of the BHM.

General Status Tab of the BHM

An example of a BHM General Status tab is displayed in Figure 74.

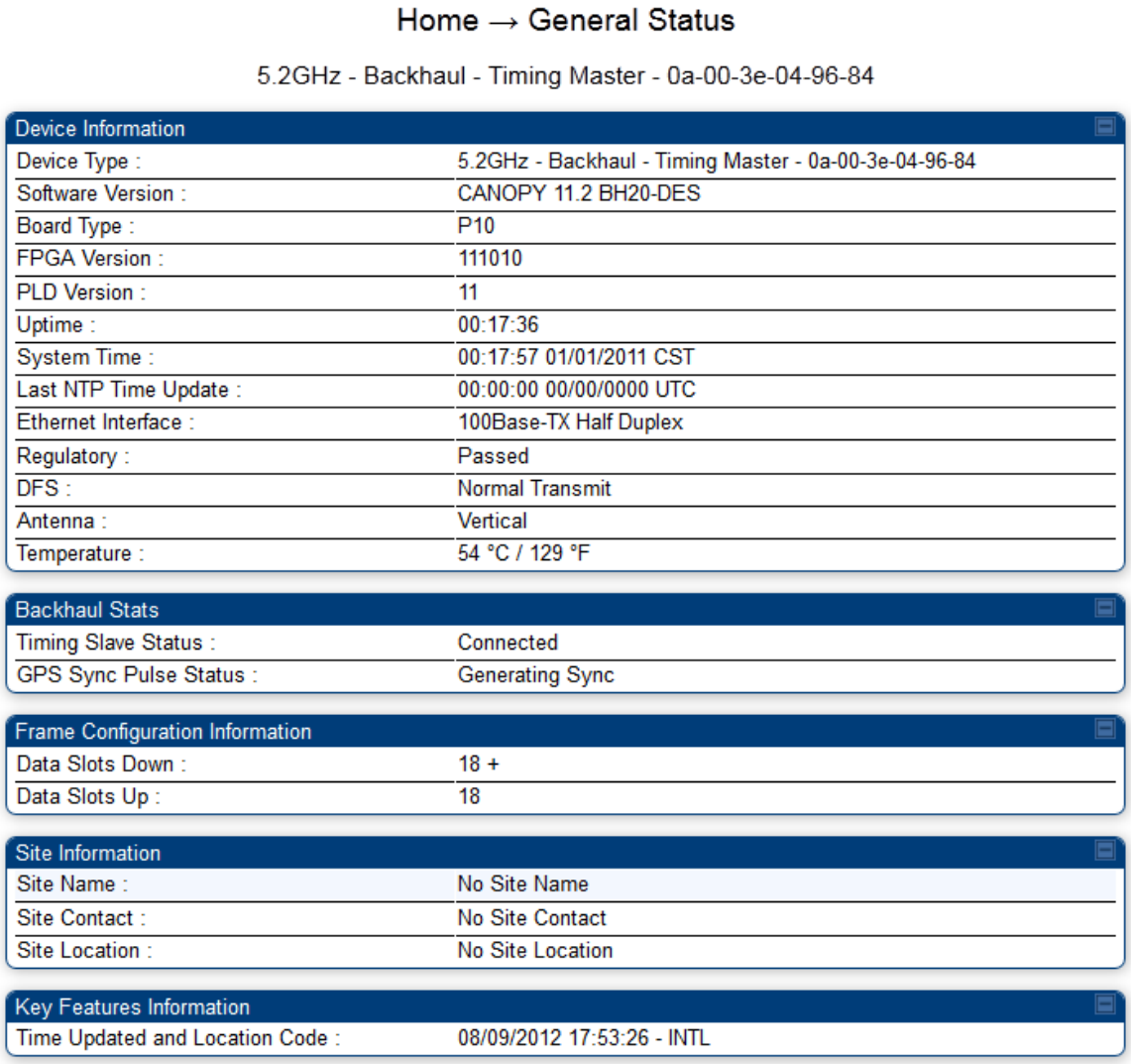

Home → General Status
5.2GHz - Backhaul - Timing Master - 0a-00-3e-04-96-84
Device Information
Device Type : 5.2GHz - Backhaul - Timing Master - 0a-00-3e-04-96-84
Software Version : CANOPY 11.2 BH20-DES
Board Type : P10
FPGA Version : 111010
PLD Version : 11
Uptime : 00:17:36
System Time : 00:17:57 01/01/2011 CST
Last NTP Time Update : 00:00:00 00/00/0000 UTC
Ethernet Interface : 100Base-TX Half Duplex
Regulatory : Passed
DFS : Normal Transmit
Antenna : Vertical
Temperature : 54 °C / 129 °F
Backhaul Stats
Timing Slave Status : Connected
GPS Sync Pulse Status : Generating Sync
Frame Configuration Information
Data Slots Down : 18 +
Data Slots Up : 18
Site Information
Site Name : No Site Name
Site Contact : No Site Contact
Site Location : No Site Location
Key Features Information
Time Updated and Location Code : 08/09/2012 17:53:26 - INTL

Figure 74: General Status tab of BHM, example

The Status page provides information on the operation of the module. This is the default web page for the module. The Status page provides the following fields.

Device Type

This field indicates the type of the module. Values include the frequency band of the module, the module type, timing mode, and the MAC address of the module.

Software Version

This field indicates the software release that is operated on the module, the release date and time of the software release, the modulation rate capability, and whether the module is secured by DES or AES encryption (see Encrypting Radio Transmissions on Page 428). When you request technical support, provide the information from this field.

Board Type

This field indicates the series of hardware. See Designations for Hardware in Radios on Page 425.

FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. If you request technical support, provide the value of this field.

PLD Version

This field indicates the version of the programmable logic device (PLD) on the module. If you request technical support, provide the value of this field.

Uptime

This field indicates how long the module has operated since power was applied.

System Time

This field provides the current time. If the BHM is connected to a CMM, then this field provides GMT (Greenwich Mean Time). The BHS that registers to the BHM inherits the system time.

Last NTP Time Update

If the Time & Date page of the module specifies that time should be received from an NTP server, then this field indicates when the time was last updated by a Network Time Protocol (NTP) server.

Ethernet Interface

If an Ethernet link to the module exists, this field indicates the speed and duplex state of the Ethernet interface to the module.

Regulatory

This field indicates whether the configured Region Code and radio frequency are compliant with respect to their compatibility. For example, you may configure a 5.4-GHz AP with a **Region Code** set to **United States** and configure a frequency that lies within the weather notch. This is a compliant combination, the radio properly operates, and its **Regulatory** field displays Passed. If later you change its Region Code to Canada, then the combination becomes non-compliant (since frequencies within the weather notch are disallowed in Canada. In this case, the radio ceases to transmit, and its **Regulatory** field displays an error message.

For further information on Region Codes and DFS, see Radar Signature Detection and Shutdown on Page 127.

DFS

This field indicates the current behavior of the radio with respect to Dynamic Frequency Selection. Possible messages in this field are

- Normal Transmit
- Radar Detected Stop Transmitting for *n* minutes, where *n* counts down from 30 to 1.
- Checking Channel Availability Remaining time *n* seconds, where *n* counts down from 60 to 1.

Antenna

The presence of this field depends on whether antenna options are available for the module. This field indicates the polarity of the antenna in the modules as one of the following:

- Horizontal
- Vertical
- External (Connectorized)

Temperature

This field displays the current operating temperature of the device (range −40°C to +55°C (−40°F to 131°F)).

Timing Slave Status

This field indicates whether this backhaul master is currently in link with a backhaul slave.

GPS Sync Pulse Status

This field indicates the status of synchronization as follows:

- **Generating sync** indicates that the module is set to *generate* the sync pulse.
- **Receiving Sync** indicates that the module is set to *receive* a sync pulse from an outside source and is receiving the pulse.
- **ERROR: No Sync Pulse** indicates that the module is set to *receive* a sync pulse from an outside source and is not receiving the pulse.

NOTE:
When this message is displayed, the BHM transmitter is turned off to avoid self-interference within the system.

Data Slots Down

This field indicates the number of frame slots that are designated for use by data traffic in the downlink (sent from the backhaul slave to the backhaul master). See Max Range on Page 249 and Downlink Data on Page 250.

Data Slots Up

This field indicates the number of frame slots that are designated for use by data traffic in the uplink (sent from the backhaul master to the backhaul slave). See Max Range on Page 249 and Downlink Data on Page 250.

Site Name

This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the BHM Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Contact

This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the BHM Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Location

This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the BHM Configuration page.

Time Updated and Location Code

This field displays information about the keying of the radio.

Concluding the Test of Point-to-Point Links

To conclude the test, perform the following steps.

Procedure 16: Verifying and recording information from the BHM

1. Confirm that the **GPS Sync Pulse Status** field indicates **Generating Sync**.
   NOTE: This indication confirms that the BHM is properly functional.
2. While your browser is set to this BHM Status page, note (or print) the values of the following fields:
   - **Device type**
   - **Software Version**
   - **Board Type**
   - **FPGA Version**
3. Systematically ensure that you can retrieve this data when you prepare to deploy the BHM.

Chapter 17: Preparing Components for Deployment

Your test of the modules not only verified that they are functional, but also yielded data that you have stored about them. Most efficiently preparing modules for deployment involves

- retrieving that data.
- systematically collecting the data into a single repository, while keeping a strong (quick) association between the data and the module.
- immediately merging module access data into this previously stored data.

Correlating Component-specific Information

You can use the data that you noted or printed from the Status pages of the modules to

- store modules for future deployment.
- know, at a glance, how well-stocked you are for upcoming network expansions.
- efficiently draw modules from stock for deployment.
- plan any software updates that you
  - wish to perform to acquire features.
  - need to perform to have the feature set be consistent among all modules in a network expansion.

You can make these tasks even easier by collecting this data into a sortable database.

Ensuring Continuing Access to the Modules

As you proceed through the steps under Configuring for the Destination on Page 236, you will set values for parameters that specify the sync source, data handling characteristics, security measures, management authorities, and other variables for the modules. While setting these, you will also tighten access to the module, specifically in

- the **Color Code** parameter of Configuration page
- the **Display-Only Access** and **Full Access** password parameters of the Configuration page.
- the addressing parameters of the IP Configuration page.

Before you set these, consider whether and how you may want to set these by a self-devised scheme. A password scheme can help you when you have forgotten or misfiled a password. An IP addressing scheme may be essential to the operation of your network and to future expansions of your network.

As you set these, note the color code and note or print the parameters you set on the Configuration page tabs. Immediately associate them with the following previously stored data about the modules:

- device type, frequency band, and MAC address
- software version and encryption type
- FPGA version

Chapter 18: Configuring for the Destination

Configuring an AP for the Destination

If an ADMINISTRATOR-level password has been set in the AP, you must log into the module before you can configure its parameters. See Managing Module Access by Passwords on Page 430.

General Tab of the AP

An example of an AP General tab is displayed in Figure 75.

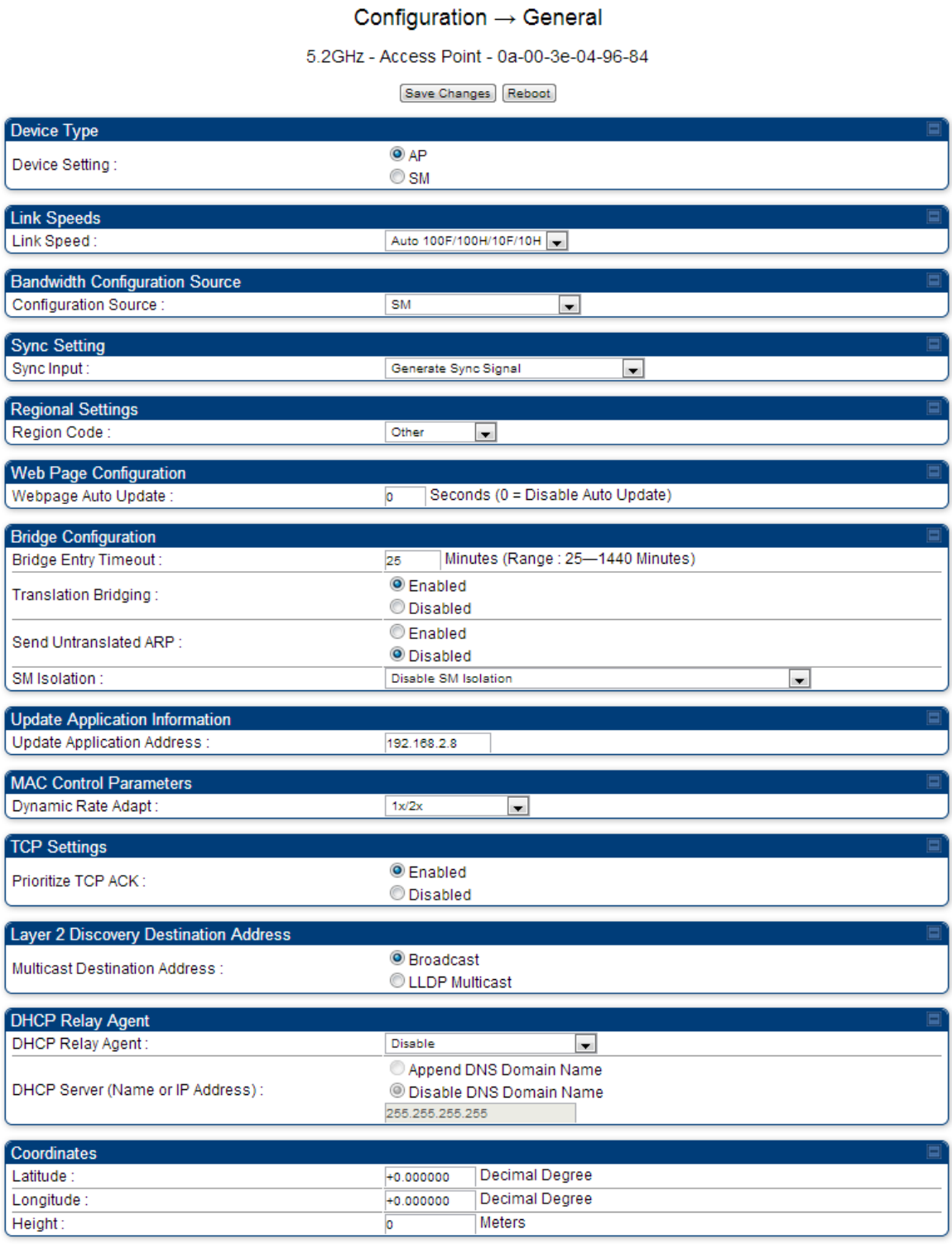


Figure 75: General tab of AP, example

The General tab of the AP contains many of the configurable parameters that define how the AP and the SMs in the sector operate. As shown in Figure 75, you may set the Configuration page parameters as follows.

Device Setting

You can temporarily transform an AP into an SM and thereby use the spectrum analyzer functionality. See Using the AP as a Spectrum Analyzer on Page 422. Otherwise, the selection for this parameter is **AP**.

Link Speeds

From the drop-down list of options, select the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected: **Auto 100F/100H/10F/10H**. In this setting, the two ends of the link automatically negotiate with each other whether the speed that they will use is 10 Mbps or 100 Mbps and whether the Ethernet traffic will be full duplex or half duplex. However, Ethernet links work best when either

- both ends are set to the same forced selection
- both ends are set to auto-negotiate and both have capability in least one common speed and traffic type combination.

Configuration Source

See Setting the Configuration Source on Page 324.

CAUTION!

Do not set this parameter to **BAM** where both

- a BAM release earlier than 2.1 is implemented.
- the **All Local SM Management** parameter (in the VLAN Configuration page of the AP) is set to **Enable**.

This combination causes the SMs to become unmanageable, until you gain direct access with an Override Plug and remove this combination from the AP configuration.

Sync Input

Specify the type of synchronization for this AP to use:

- Select **Sync to Received Signal (Power Port)** to set this AP to receive sync from a connected CMMmicro or CMM4.
- Select **Sync to Received Signal (Timing Port)** to set this AP to receive sync from a connected CMM2, an AP in the cluster, an SM, or a BH timing slave.

- Select **Generate Sync Signal** where the AP does not receive sync, and no other AP or BHM is active within the link range.

Verify GPS Message Checksum

When enabled (Sync Input "Sync to Received Signal (Timing Port)" must be selected for this parameter to display), the device validates GPS messaging to ensure that the radio is properly receiving data from the GPS source. If a GPS source is not calculating and sending checksum data properly, the AP will still receive synchronization pulses but not GPS data (location, data, etc.) and the Invalid Message counter will increase on the radio's Home > GPS Status page. If an AP is receiving synchronization properly from a GPS unit but is not receiving GPS data, operators may set **Verify GPS Message Checksum** to "Disabled" to ignore checksum failures and to allow the AP to process the GPS data.

Region Code

From the drop-down list, select the region in which the radio is operating.
When the appropriate region is selected in this parameter, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard. For further information on DFS, see Radar Signature Detection and Shutdown on Page 127.

Unlike selections in other parameters, your **Region Code** selection requires a **Save Changes** and a **Reboot** cycle before it will force the context-sensitive GUI to display related options (for example, **Alternate Frequency Carrier *1 and 2*** in the Configuration => Radio tab). Thus, a proper configuration exercise in environments that are subject to DFS requirements has two imperative **Save Changes** and **Reboot** cycles: one after the **Region Code** is set, and a second after related options are set.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

Bridge Entry Timeout

Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.

CAUTION!
An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.

Translation Bridging

If you want the Translation Bridging feature, select **Enabled**. This has numerous implications. For a full description of them, see Uplink Frame on Page 81.

Send Untranslated ARP

If the **Translation Bridging** parameter is set to **Enabled**, then the **Send Untranslated ARP** parameter can be

- disabled, so that the AP will overwrite the MAC address in Address Resolution Protocol (ARP) packets before forwarding them.
- enabled, so that the AP will forward ARP packets regardless of whether it has overwritten the MAC address.

See Uplink Frame on Page 81 and Address Resolution Protocol on Page 164.

If the **Translation Bridging** parameter is set to **Disabled**, then the **Send Untranslated ARP** parameter has no effect.

SM Isolation

Prevent or allow SM-to-SM communication by selecting from the following drop-down menu items:

- **Disable SM Isolation** (the default selection). This allows full communication between SMs.
- **Block SM Packets from being forwarded**. This prevents both multicast/broadcast and unicast SM-to-SM communication.
- **Block and Forward SM Packets to Backbone**. This not only prevents multicast/broadcast and unicast SM-to-SM communication but also sends the packets, which otherwise would have been handled SM to SM, through the Ethernet port of the AP.

Update Application Address

Enter the address of the server to access for software updates on this AP and registered SMs.

Dynamic Rate Adapt

This parameter is present in only PMP 100 Series APs. You should generally keep this parameter set to **1x/2x** to allow the module to automatically the operation rate. For troubleshooting, you may lock the rate down (Disabled), but be aware that this locks down the operation rate for all uplinks and downlinks across the sector. See 2X Operation on Page 89.

Prioritize TCP ACK

To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements. This parameter, when enabled, can be particularly useful when running bi-direction FTP sessions over the link. If a link is primarily used for video surveillance, it is recommended to configure this parameter to "Disabled". See AP-SM Links on Page 99.

Multicast Destination Address

Using Link Layer Discovery Protocol (LLDP), a module exchanges multicast addresses with the device to which it is wired on the Ethernet interface. Although some switches (CMMmicro, for example) do not pass LLDP addresses upward in the network, a radio can pass it as the value of the **Multicast Destination Address** parameter value in the connected device that has it populated.

In this way, an SM can report to Prizm, for example, the multicast address of a connected remote AP, and thus allow Prizm to discover that AP. To allow this, set the message mode in the remote AP to **LLDP Multicast**. The SM will pass this address in broadcast mode, and the CMMmicro will pass the address upward in the network, since it does not discard addresses that it receives in broadcast mode.

Where the AP is not behind another device, the **Broadcast** mode will allow discovery of the AP.

DHCP Relay Agent

The AP may act as a DHCP relay for SMs and CPEs underneath it. The AP will make use of the DHCP Option 82 (DHCP Relay Agent Information) from RFC 3046 when performing relay funtions. The AP offers two types of DHCP relay functionality:

- **Full Relay Information**. Configuring the DHCP Full Relay Operation will take broadcast DHCP packets and send them to a Unicast server in unicast mode. This way the DHCP requests and replies can be routed like any other UDP packet.
- **Only Insert Option 82**. This option leaves the DHCP request on its broadcast domain as opposed to DHCP Full Relay Operation which will turn it into a unicast packet.

In order to accommodate setting up pools or classes for different VLANs, the Option 82 field will include information to tell the server what VLAN the client is on.

DHCP Server (Name or IP Address)

This field represents the DHCP server for which DHCP messaging relayed for SMs and CPEs situated beneath the AP. The DHCP relay server may be either a DNS name or a static IP address in dotted decimal notation. Additionally the management DNS domain name may be toggled such that the name of the DHCP relay server only needs to be specified and the DNS domain name is automatically appended to that name. The default DHCP relay server addresses is 255.255.255.255 with the appending of the DNS domain name disabled.

Coordinates

Physical radio location data may be configured via the **Latitude**, **Longitude**, and **Height** fields.

Save Changes

When you click this button, any changes that you made on the this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

- the module reboots.
- any changes that you saved by a click of the **Save Changes** button are implemented.

IP Tab of the AP

An example of the IP tab of the AP is displayed in Figure 76.

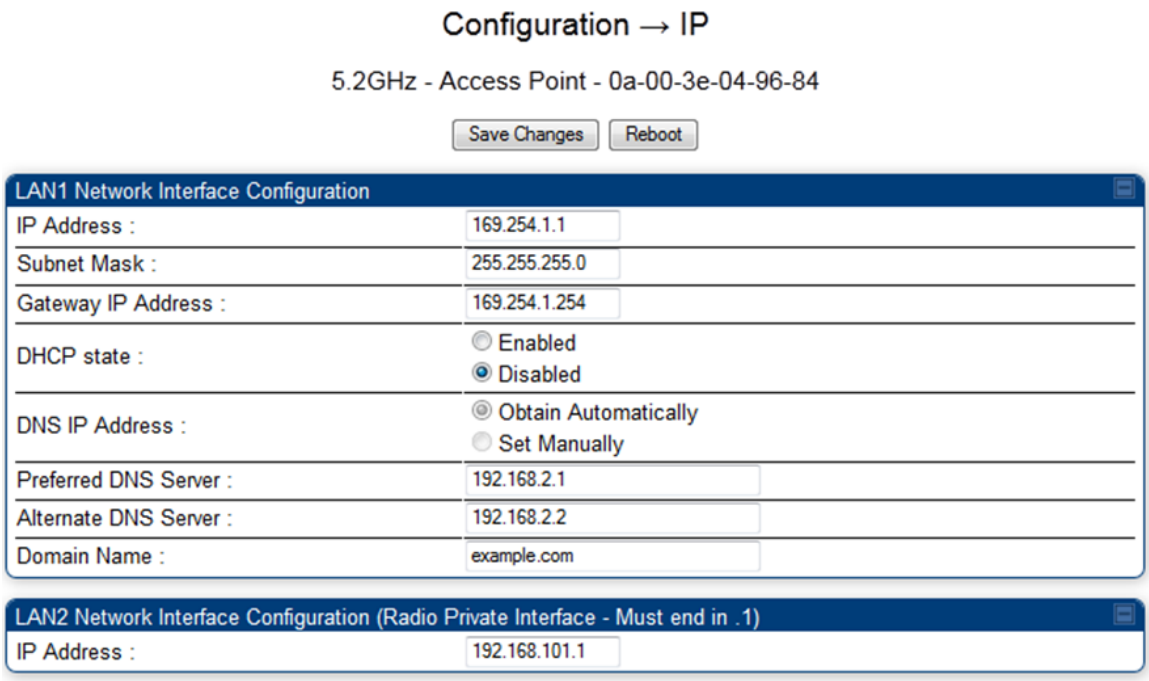


Figure 76: IP tab of AP, example

You may set the IP tab parameters as follows.

LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to associate with the Ethernet connection on this AP. (The default IP address from the factory is 169.254.1.1.) If you set and then forget this parameter, then you must both

- physically access the module.
- use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 433.

RECOMMENDATION:
Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the AP to communicate on the network. The default subnet mask is 255.255.0.0. See Allocating Subnets on Page 164.

LAN1 Network Interface Configuration, Gateway IP Address

Enter the appropriate gateway for the AP to communicate with the network. The default gateway is 169.254.0.0.

The values of these four LAN1 network interface configuration parameters are displayed read only along with the Ethernet speed and duplex state on the Network Interface tab of the Home page in the AP.

LAN1 Network Interface Configuration, DHCP State

If you select **Enabled**, the DHCP server automatically assigns the IP configuration (IP address, subnet mask, and gateway IP address) and the values of those individual parameters (above) are not used. The setting of this DHCP state parameter is also viewable, but not settable, in the Network Interface tab of the Home page.

DNS IP Address

Canopy devices allow for configuration of a preferred and alternate DNS server IP address either automatically or manually. Devices must set DNS server IP address manually when DHCP is disabled for the management interface of the device. DNS servers may be configured automatically from the DHCP response when DHCP is enabled for the management interface of the device. Optionally devices may be configured to set the DNS server IP address manually when DHCP is enabled for the management interface. The default DNS IP addresses are 0.0.0.0 when configured manually.

Preferred DNS Server

The first address used for DNS resolution.

Alternate DNS Server

Upon failure to reach the Preferred DNS Server, the Alternate DNS Server is used.

Domain Name

The operator's management domain name may be configured for DNS. The domain name configuration can be used for configuration of the servers in the operator's network. The default domain name is example.com, and is only used if configured as such.

LAN2 Network Interface Configuration (RF Private Interface), IP Address

You should not change this parameter from the default *AP* private IP address of 192.168.101.1. A /24 CIDR subnet is used to communicate with each of the SMs that are registered. The AP uses a combination of the private IP and the LUID (logical unit ID) of the SM.

For example, if an SM is the first to register in an AP, and another SM registers later, then the AP whose Private IP address is 192.168.101.1 uses the following *SM* Private IP addresses to communicate to each:

SM	LUID	Private IP
First SM registered	2	192.168.101.2
Second SM registered	3	192.168.101.3

NOTE:
Where space is limited for subnet allocation, be advised that an SM *need not* have an operator-assigned IP address. The SM is directly accessible without an LUID if either the SM **Color Code** parameter is set to 0 or the AP has a direct Ethernet connection to the SM.

The IP Configuration page also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Radio Tab of the AP

An example of the Radio tab of the AP is shown in Figure 77.

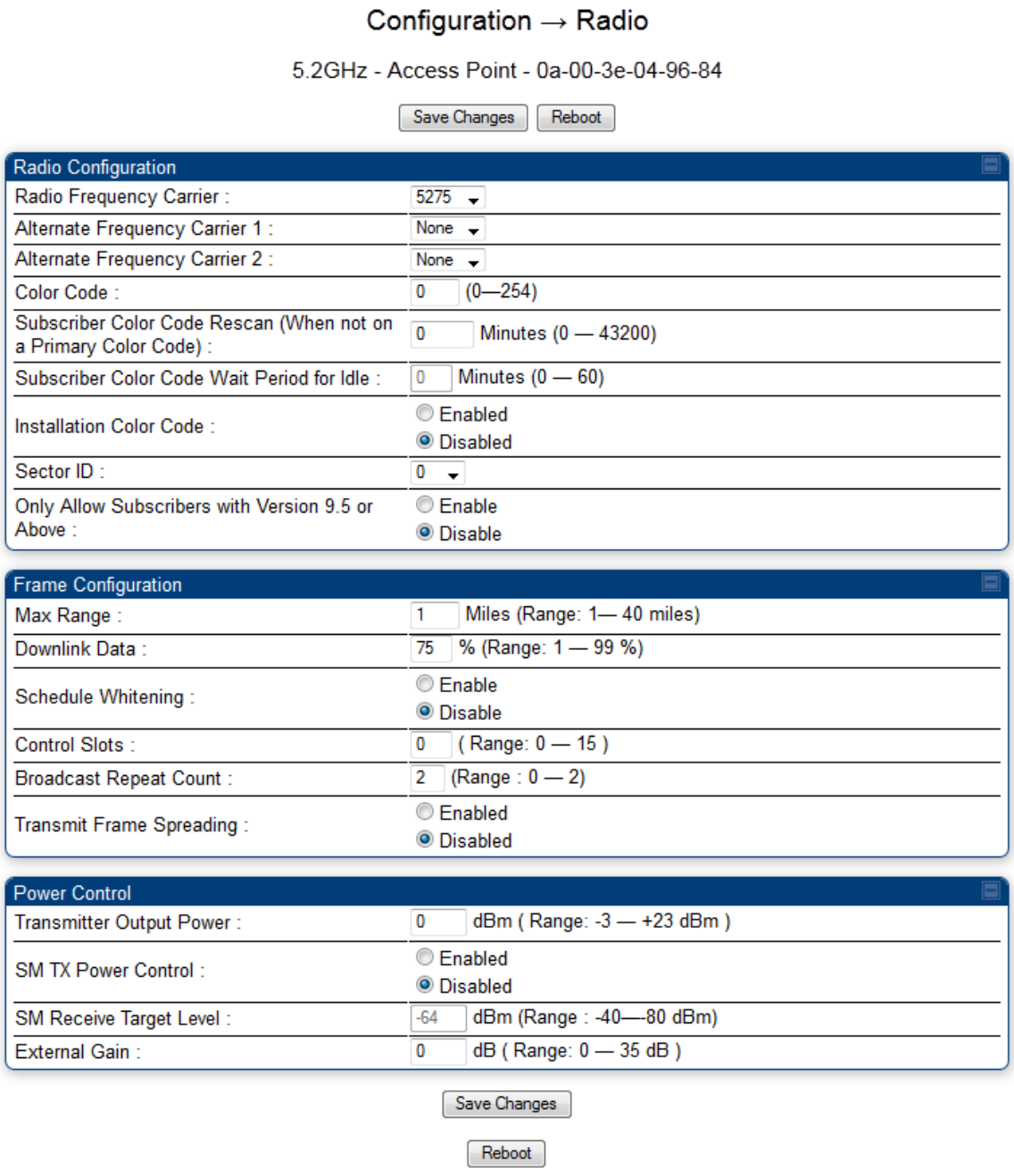

Configuration → Radio
5.2GHz - Access Point - 0a-00-3e-04-96-84
Save Changes
Reboot
Radio Configuration
Radio Frequency Carrier : 5275
Alternate Frequency Carrier 1 : None
Alternate Frequency Carrier 2 : None
Color Code : 0 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) : 0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle : 0 Minutes (0 — 60)
Installation Color Code : Enabled Disabled
Sector ID : 0
Only Allow Subscribers with Version 9.5 or Above : Enable Disable
Frame Configuration
Max Range : 1 Miles (Range: 1— 40 miles)
Downlink Data : 75 % (Range: 1 — 99 %)
Schedule Whitening : Enable Disable
Control Slots : 0 (Range: 0 — 15)
Broadcast Repeat Count : 2 (Range : 0 — 2)
Transmit Frame Spreading : Enabled Disabled
Power Control
Transmitter Output Power : 0 dBm (Range: -3 — +23 dBm)
SM TX Power Control : Enabled Disabled
SM Receive Target Level : -64 dBm (Range : -40—-80 dBm)
External Gain : 0 dB (Range: 0 — 35 dB)
Save Changes
Reboot

Figure 77: Radio tab of AP, example

The Radio tab of the AP contains some of the configurable parameters that define how the AP operates. You may set the Radio tab parameters as follows.

Radio Frequency Carrier

Specify the frequency for the module to transmit. The default for this parameter is **None**. (The selection labeled **Factory** requires a special software key file for implementation.) For a list of channels in the band, see the drop-down list or Considering Frequency Band Alternatives on Page 134.

Alternate Frequency Carrier 1

If your network operates in a region in which DFS shutdown capability is required, and you do not see this parameter, perform the following steps:

1. Click the General tab.
2. Set the **Region Code** parameter from its drop-down list.
3. Click the **Save Changes** button.
4. Click the **Reboot** button.
5. Click the Radio tab.

From the drop-down list, select the frequency that the AP should switch to if it detects a radar signature on the frequency configured in the **Radio Frequency Carrier** parameter. See Radar Signature Detection and Shutdown on Page 127.

Alternate Frequency Carrier 2

From the drop-down list, select the frequency that the AP should switch to if it detects a radar signature on the frequency configured in the **Alternate Frequency Carrier 1** parameter. See Radar Signature Detection and Shutdown on Page 127.

Color Code

Specify a value from 0 to 254. For registration to occur, the color code of the SM and the AP *must* match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code.

Color code allows you to force an SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).

RECOMMENDATION:
Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

Subscriber Color Code Rescan (When not on a Primary Color Code)

This timer may be utilized to initiate SM rescans in order to register to an AP configured with the SM's primary color code.

The time (in minutes) for a subscriber to rescan (if this AP is not configured with the SM's primary color code). This timer will only fire once – if the **Subscriber Color Code Wait Period for Idle** timer is configured with a nonzero value and the **Subscriber Color Code Rescan** expires, the **Subscriber Color Code Wait Period for Idle** will be started. If the **Subscriber Color Code Wait Period for Idle** timer is configured with a zero value and the **Subscriber Color Code Rescan** timer expires, the SM will immediately go into rescan mode.

Subscriber Color Code Wait Period for Idle

The time (in minutes) for a subscriber to rescan while idle (if this AP is not configured with the SM's primary color code). This timer will fire periodic events. The fired event determines if any RF unicast traffic (either inbound or outbound) has occurred since the last event. If the results of the event determine that no RF unicast traffic has occurred (SM is idle), then the subscriber will rescan.

Installation Color Code

With this feature enabled on the AP and SM, operators may install and remotely configure SMs without having to configure matching color codes between the modules. While the SM is accessible for configuration from above the AP (for remote provisioning) and below the SM (for local site provisioning), no user data is passed over the radio link. When using the Installation Color Code feature, ensure that the SM is configured with the factory default Color Code configuration (Color Code 1 is "0", Color Code 2-10 set to "0" and "Disable"). The status of the Installation Color Code can be viewed on the AP Eval web GUI page, and when the SM is registered using the Installation Color Code the message "SM is registered via ICC – Bridging Disabled!" is displayed in red on every SM GUI page. The Installation Color Code parameter is configurable without a radio reboot for both the AP and SM. If an SM is registered via Installation Color Code and the feature is then disabled, operators will need to reboot the SM or force it to reregister (i.e. using the **Rescan APs** functionality on the AP Eval page).

Power Save Mode

P10 Board Types Only - Select either

- **Enabled** (the default), to reduce module power consumption by approximately 10% without affecting the transmitter output power. This is the recommended setting.
- **Disabled**, to continue normal power consumption, but do so only under guidance from technical support.

Sector ID

Specify a number in the range 1 to 6 to associate with this AP. The Sector ID setting does not affect the operation of the AP. On the AP Evaluation tab of the Tools page in the SM, the **Sector ID** field identifies the AP that the SM sees. The following steps may be useful:

- Assign a unique Sector ID to each sector in an AP cluster.
- Repeat the assignment pattern throughout the entire system.

Only Allow Subscribers with Version 9.5 or Above

For feature compatibility, an operator may enforce that all SMs in a sector are running Software Release 9.5 or above. If an SM that is running pre-9.5 software tries to register to an AP with this option enabled, it will be rejected and an SM registration failure trap will be sent indicating why the SM was not allowed to register.

Max Range

Enter a number of miles (or kilometers divided by 1.61, then rounded to an integer) for the furthest distance from which an SM is allowed to register to this AP. Do not set the distance to any greater number of miles. A greater distance

- does not increase the power of transmission from the AP.
- can reduce aggregate throughput. See Table 24 on Page 100.

Regardless of this distance, the SM must meet the minimum requirements for an acceptable link. If the AP is in cluster, then you *must* set this parameter on all other APs in the cluster exactly the same, except as described in the NOTE admonition below. The default value of this parameter is 2 miles (3.2 km).

For APs in the non 900-MHz frequency band ranges, although the typical maximum range where an SM is deployed with a reflector is 15 miles (24 km), you can set this parameter to as far as 30 miles (48 km). Without increasing the power or sensitivity of the AP or SM, the greater value allows you to attempt greater distance where the RF environment and Fresnel zone[6] are especially clear.

For the PMP 400 Series AP, the typical maximum range achievable depends on the operation mode as follows:

- 5 miles (8 km) in 1X operation
- 2.5 miles (4 km) in 2X operation
- 1.25 miles (2 km) in 3X operation

A value of 15 for this parameter decreases the number of available data slots by 1. With a higher value, the number is further decreased as the AP compensates for the expected additional air delay.

[6] See Noting Possible Obstructions in the Fresnel Zone on Page 136.

Downlink Data

Specify the percentage of the aggregate throughput for the downlink (frames transmitted from the AP to the subscriber). For example, if the aggregate (uplink and downlink total) throughput on the AP is 6 Mb, then 75% specified for this parameter allocates 4.5 Mb for the downlink and 1.5 Mb for the uplink. The default for this parameter is 75%.

CAUTION!
You must set this parameter exactly the same for all APs in a cluster.

Schedule Whitening

Select either

- **Enable**, to spread the transmitted signal power to avoid peaks that modules with Dynamic Frequency Selection (DFS) configured might interpret as radar. This is the recommended setting.
- **Disable**, to allow peaks in transmitted signal power.

PMP 400 Series OFDM APs do not have this parameter.

Control Slots

Field results have indicated that, in general, systems perform better with a slightly higher number of control slots than previously recommended. If you are experiencing latency or SM-servicing issues, increasing the number of control slots may increase system performance, depending on traffic mix over time.

Use care when changing the control slot configuration of only some APs, because changes affect the uplink/downlink ratio and can cause co-location issues. For APs in a cluster of mismatched control slots settings, or where OFDM and FSK AP of the same frequency band are co-located, use the frame calculator. See Using the Frame Calculator Tool (All) for Co-location on Page 542.

CAUTION!
Change control slot configuration in an operating, stable system cautiously and with a back-out plan. After changing a control slot configuration, monitor the system closely for problems as well as improvements in system performance.

The recommended number of control slots is as stated in Table 49 or Table 50.

Table 49: Control slot settings for all FSK APs in cluster

Number of High Priority Channel Disabled SMs that Register to the AP	Number of Control Slots Recommended
1 to 10	1
11 to 50	2
51 to 150	4
151 to 200	6

Table 50: Control slot settings for all OFDM APs in cluster

Number of High Priority Channel Disabled SMs that Register to the AP	Number of Control Slots Recommended
1 to 10	2
11 to 50	4
51 to 150	6
151 to 200	8

This field indicates the number of (reserved) control slots configured by the operator. Control slots are half the size of data slots. The SM uses reserved control slots and unused data slots for bandwidth requests. SMs with High Priority Channel use an additional Virtual Circuit, and should be counted twice when planning Control Slot configuration. For example, a network including 20 SMs with High Priority Channel disabled and 20 SMs with High Priority Channel enabled may be configured with 4 Control Slots (this is a recommendation based on the number of SMs in the network – see below for other factors contributing to Control Slot configuration decisions).

If too few reserved control slots are specified, then latency increases in high traffic periods. If too many are specified, then the maximum capacity is unnecessarily reduced.

In a typical cluster, each AP should be set to the same number of control slots to assure proper timing in the send and receive cycles. However, where high incidence of small packets exists, as in a sector that serves several VoIP streams, additional control slots may provide better results. For APs in a cluster of mismatched control slots settings, or where OFDM and FSK APs of the same frequency band are co-located, use the frame calculator. See Using the Frame Calculator Tool (All) for Co-location on Page 542.

Broadcast Repeat Count

The default is 2 repeats (in addition to the original broadcast packet, for a total of 3 packets sent for every one needed), and is settable to 1 or 0 repeats (2 or 1 packets for every broadcast).

ARQ (Automatic Repeat reQuest) is not present in downlink broadcast packets, since it would cause unnecessary uplink traffic from every SM for each broadcast packet. For successful transport without ARQ, the AP repeats downlink broadcast packets. The SMs filter out all repeated broadcast packets and, thus, do not transport further.

The default of 2 repeats is optimum for typical uses of the network as an internet access system. In applications with heavy download broadcast such as video distribution, overall throughput is significantly improved by setting the repeat count to 1 or 0. This avoids flooding the downlink with repeat broadcast packets.

External Filters Delay

This parameter is present in only 900-MHz modules and can have effect in only those that have interference mitigation filter(s). Leave this value set to **0**, regardless of whether the AP has an interference mitigation filter.

Transmit Frame Spreading

The following description applies to APs in frequency ranges *other than* 900-MHz.

Where multiple AP clusters operate in the same frequency band range and same geographical area, select **Enable**. Then SMs between two APs can register in the assigned AP (do not register in another AP).

Where multiple AP clusters *do not* operate in the same frequency band range and same geographical area, select **Disable**, but observe the following caveat.

IMPORTANT!

SM throughput is 10% greater with this feature disabled. However, if you disable **Transmit Frame Spreading** where this feature was previously enabled, monitor the zone for interference over a period of days to ensure that this action has not made any SMs sensitive to the wrong beacon.

With this selection enabled, the AP does not transmit a beacon in each frame, but rather transmits a beacon in only pseudo-random frames in which the SM expects the beacon. This allows multiple APs to send beacons to multiple SMs in the same range without interference.

Transmitter Output Power

Nations and regions may regulate transmitter output power. For example

- 900-MHz, 2.4-GHz, and 5.7-GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance.
- Legal maximum allowable transmitter output power and EIRP (Equivalent Isotropic Radiated Power) in the 2.4-GHz frequency band varies by country and region. The output power of Series P9 2.4-GHz modules can be adjusted to meet these national or regional regulatory requirements.

- Countries and regions that permit the use of the 5.4-GHz frequency band (CEPT member states, for example), generally require equipment using the band to have adjustable power. In the 5.4-GHz PMP 400 Series OFDM AP, transmitter output power is settable in the range of −30 to 15 dBm. However, with only the integrated antenna, where regulation[7] requires that EIRP is not greater than 27 dBm, compliance requires that the transmitter output power is set to 10 dBm or less. With a 12 dBi external antenna on the connectorized version of this AP, the full range (up to 15 dBm) is acceptable.

The professional installer of the equipment has the responsibility to

- maintain awareness of applicable regulations.
- calculate the permissible transmitter output power for the module.
- confirm that the initial power setting is compliant with national or regional regulations.
- confirm that the power setting is compliant following any reset of the module to factory defaults.

For information on how to calculate the permissible transmitter output power to enter in this parameter, see Adjusting Transmitter Output Power on Page 382.

SM TX Power Control

An AP can control registered SMs' transmit power level such that a desired receive target power is seen at the AP. This feature is useful in DFS regions so that signals from close-in SMs are not being received at excessively high power levels which may cause the AP to false detect. It is also useful for managing the general RF environment and controlling effective sector size by ensuring that SMs don't transmit at any higher power than required. The **SM TX Power Control** option is only available on PMP 100 APs which are Transmit Power Control (TPC) capable. This includes all series P10 and P11 PMP 100 (FSK) radios as well as some P9 radios that have adjustable power (instead of Normal/Low Power). All 900-MHz radios are TPC capable. Likewise, only SMs that are TPC capable will be able to use SM power control. If SM power control is enabled on an AP and an SM which is not TPC capable connects to that AP, it will ignore any power adjust requests and will operate as it did prior to Release 10.5. Also, any SMs which are not upgraded to Release 10.5 will ignore any power adjust requests and will operate with fixed power as set by the operator.

SM Receive Target Level

Each SM's Transmitter Output Power is automatically set by the AP. The AP monitors the received power from each SM, and adjusts each SM's Transmitter Output Power so that the received power at the AP from that SM is not greater what is set in this field. This value represents a "single-port" power perceived on the SM.

[7] This is the case in most regions, including the U.S.A., Europe, and Canada.

External Gain

If your network operates in a region in which DFS shutdown capability is required, and you do not see this parameter, perform the following steps:

1. Click the General tab.
2. Set the **Region Code** parameter from its drop-down list.
3. Click the **Save Changes** button.
4. Click the **Reboot** button.
5. Click the Radio tab.

Using Table 51 as a guide, type in the dB value by which to reduce Dynamic Frequency Selection (DFS) sensitivity to radar signals.

Table 51: Recommended External Gain values for AP

Module Type	Recommended Setting
FSK with only integrated patch antenna	0
FSK with 9 dB Canopy LENS	9
FSK with standard 18 dB reflector	18
FSK connectorized with 15.5 dBi antenna and 0.5 dB cable loss	15
OFDM with only integrated antenna	17
OFDM connectorized with antenna that was purchased with it	17
OFDM connectorized with separately purchased antenna	antenna gain minus coax + connector loss

The value of this parameter does not affect transmitter output power. This parameter is present in only radios that support DFS and hence is not present in 900-MHz radios.

The Radio tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

SNMP Tab of the AP

An example of the SNMP tab of the AP is displayed in Figure 78.

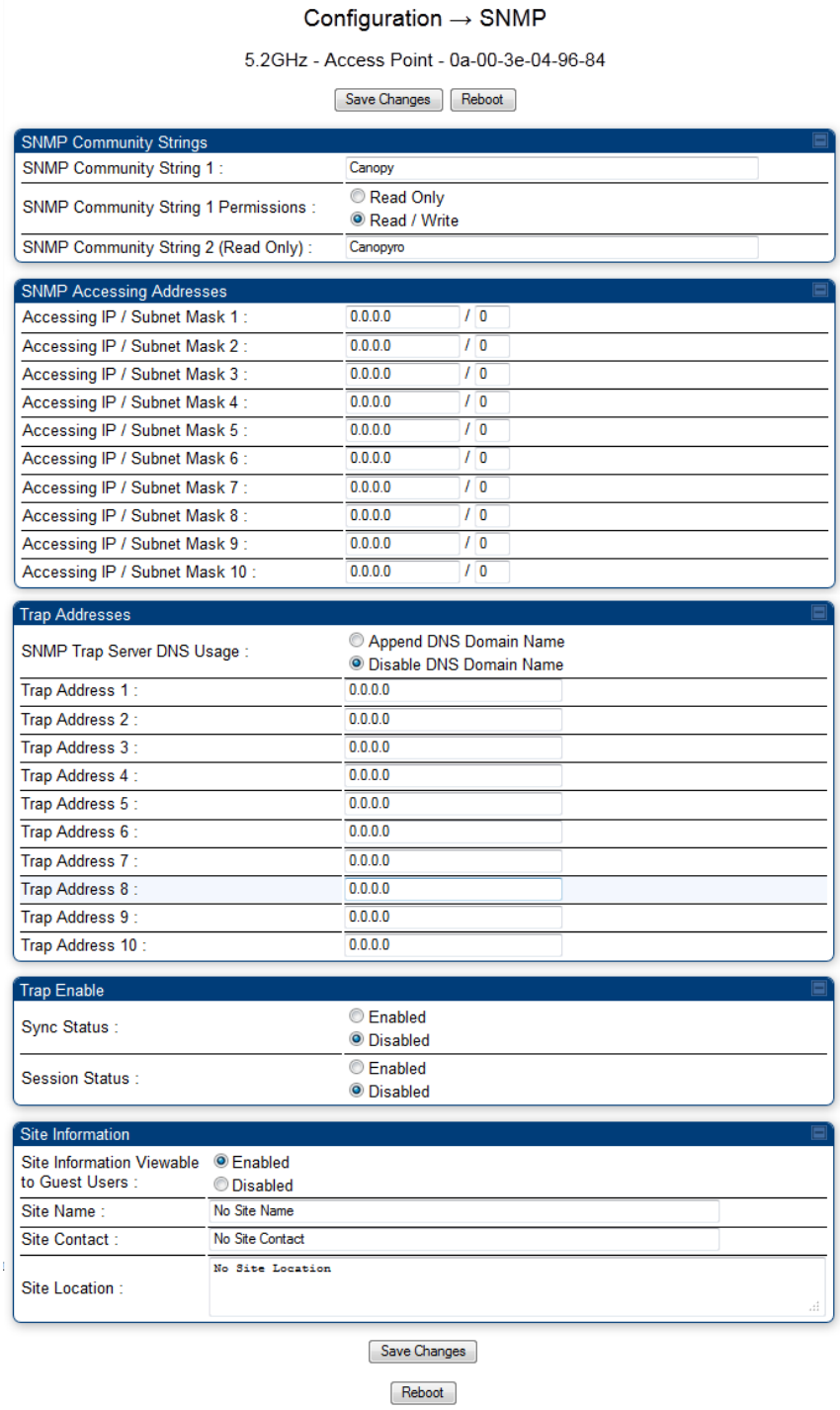

Configuration → SNMP
5.2GHz - Access Point - 0a-00-3e-04-96-84
Save Changes
Reboot
SNMP Community Strings
SNMP Community String 1 :
Canopy
SNMP Community String 1 Permissions :
Read Only
Read / Write
SNMP Community String 2 (Read Only) :
Canopyro
SNMP Accessing Addresses
Accessing IP / Subnet Mask 1 :
Accessing IP / Subnet Mask 2 :
Accessing IP / Subnet Mask 3 :
Accessing IP / Subnet Mask 4 :
Accessing IP / Subnet Mask 5 :
Accessing IP / Subnet Mask 6 :
Accessing IP / Subnet Mask 7 :
Accessing IP / Subnet Mask 8 :
Accessing IP / Subnet Mask 9 :
Accessing IP / Subnet Mask 10 :
0.0.0.0 / 0
Trap Addresses
SNMP Trap Server DNS Usage :
Append DNS Domain Name
Disable DNS Domain Name
Trap Address 1 :
Trap Address 2 :
Trap Address 3 :
Trap Address 4 :
Trap Address 5 :
Trap Address 6 :
Trap Address 7 :
Trap Address 8 :
Trap Address 9 :
Trap Address 10 :
0.0.0.0
Trap Enable
Sync Status :
Enabled
Disabled
Session Status :
Site Information
Site Information Viewable to Guest Users :
Site Name :
No Site Name
Site Contact :
No Site Contact
Site Location :
No Site Location

Figure 78: SNMP tab of AP, example

You may set the SNMP tab parameters as follows.

SNMP Community String 1

Specify a control string that can allow an Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is **Canopy**.

SNMP Community String 1 Permissions

You can designate the **SNMP Community String 1** to be the password for Prizm, for example, to have read/write access to the module via SNMP, or for all SNMP access to the module to be read only.

SNMP Community String 2 (Read Only)

Specify an additional control string that can allow an Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. The default string is **Canopy2**. This password will never authenticate a user or an NMS to read/write access.

The **Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **Accessing Subnet**, **Trap Address**, and **Permission** parameters.

Accessing IP / Subnet Mask *1 to 10*

Specify the addresses that are allowed to send SNMP requests to this AP. The NMS has an address that is among these addresses (this subnet). You must enter both

- The network IP address in the form xxx.xxx.xxx.xxx
- The CIDR (Classless Interdomain Routing) prefix length in the form /xx

For example

- the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).
- 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the AP, presuming that the device supplies the correct **Community String** value.

The default treatment is to allow all networks access. For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.” You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations.

SNMP Trap Server DNS Usage

The management DNS domain name may be toggled such that the name of the trap server only needs to be specified and the DNS domain name is automatically appended to that name. The default SNMP trap server addresses for all 10 available servers is 0.0.0.0 with the appending of the DNS domain name disabled.

Trap Address *1 to 10*

Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) to which SNMP traps should be sent. Traps inform Prizm or an NMS that something has occurred. For example, trap information is sent

- after a reboot of the module.
- when an NMS attempts to access agent information but either
  - supplied an inappropriate community string or SNMP version number.
  - is associated with a subnet to which access is disallowed.

Trap Enable, Sync Status

If you want sync status traps (sync lost and sync regained) sent to Prizm or an NMS, select **Enabled**. If you want these traps suppressed, select **Disabled**.

Trap Enable, Session Status

If you want session status traps sent to Prizm or an NMS, select **Enabled**. For the names and descriptions of session status traps, see Traps Provided in the Canopy Enterprise MIB on Page 497. If you want these traps suppressed, select **Disabled**.

Site Information Viewable to Guest Users

Operators can enable or disable site information from appearing when a user is in GUEST account mode.

Site Name

Specify a string to associate with the physical module. This parameter is written into the *sysName* SNMP MIB-II object and can be polled by PrizmEMS or an NMS. The buffer size for this field is 128 characters.

Site Contact

Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by PrizmEMS or an NMS. The buffer size for this field is 128 characters.

Site Location

Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by PrizmEMS or an NMS. The buffer size for this field is 128 characters.

The SNMP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Quality of Service (QoS) Tab of the AP

An example of the Quality of Service (QoS) tab of the AP is displayed in Figure 79.

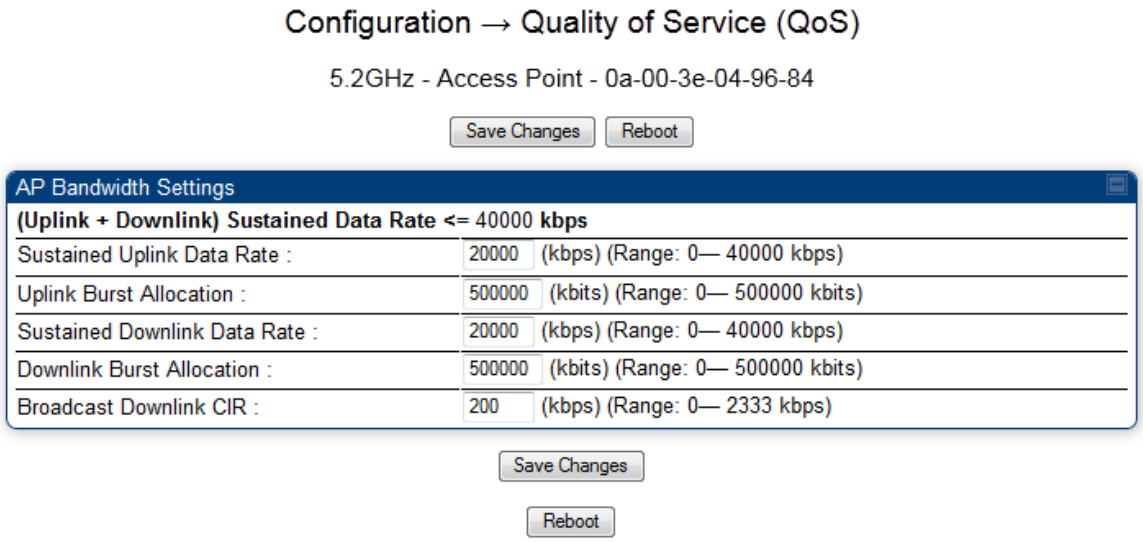

Configuration → Quality of Service (QoS)
5.2GHz - Access Point - 0a-00-3e-04-96-84
Save Changes
Reboot
AP Bandwidth Settings
(Uplink + Downlink) Sustained Data Rate <= 40000 kbps
Sustained Uplink Data Rate : 20000 (kbps) (Range: 0— 40000 kbps)
Uplink Burst Allocation : 500000 (kbits) (Range: 0— 500000 kbits)
Sustained Downlink Data Rate : 20000 (kbps) (Range: 0— 40000 kbps)
Downlink Burst Allocation : 500000 (kbits) (Range: 0— 500000 kbits)
Broadcast Downlink CIR : 200 (kbps) (Range: 0— 2333 kbps)
Save Changes
Reboot

Figure 79: Quality of Service (QoS) tab of AP, example

In the Quality of Service (QoS) tab, you may set AP bandwidth parameters as follows.

Sustained Uplink Data Rate

Specify the rate that each SM registered to this AP is replenished with credits for transmission. This default imposes no restriction on the uplink. See

- Maximum Information Rate (MIR) Parameters on Page 83
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 86
- Setting the Configuration Source on Page 324.

Uplink Burst Allocation

Specify the maximum amount of data to allow each SM to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more. See

- Maximum Information Rate (MIR) Parameters on Page 83
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 86
- Setting the Configuration Source on Page 324.

Sustained Downlink Data Rate

Specify the rate at which the AP should be replenished with credits (tokens) for transmission to each of the SMs in its sector. This default imposes no restriction on the uplink. See

- Maximum Information Rate (MIR) Parameters on Page 83
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 86
- Setting the Configuration Source on Page 324.

Downlink Burst Allocation

Specify the maximum amount of data to allow the AP to transmit to any registered SM before the AP is replenished with transmission credits at the **Sustained Downlink Data Rate**. See

- Maximum Information Rate (MIR) Parameters on Page 83
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 86
- Setting the Configuration Source on Page 324.

Broadcast Downlink CIR

Broadcast Downlink CIR (Committed Information Rate, a minimum) supports some system designs where downlink broadcast is desired to have higher priority than other traffic. For many other system designs, especially typical internet access networks, leave the Broadcast Downlink CIR at the default.

Broadcast Downlink CIR is closely related to the Broadcast Repeat Count parameter, which is settable in the Radio tab of the Configuration page in the AP: when the Broadcast Repeat Count is changed, the total of available bandwidth is also changed, since packets are being sent one, two, or three times, according to the setting in the Broadcast Repeat Count parameter. (See Broadcast Repeat Count on Page 251.)This relationship is shown in Table 52.

Table 52: Broadcast Downlink CIR achievable per Broadcast Repeat Count

Broadcast Repeat Count	Number of times each packet is sent	Highest Achievable Value for Broadcast Downlink CIR
0	1	7000 kbps
1	2	3500 kbps
2	3	2333 kbps

The Quality of Server (QoS) tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Security Tab of the AP

An example of the Security tab of the AP is displayed in Figure 80.

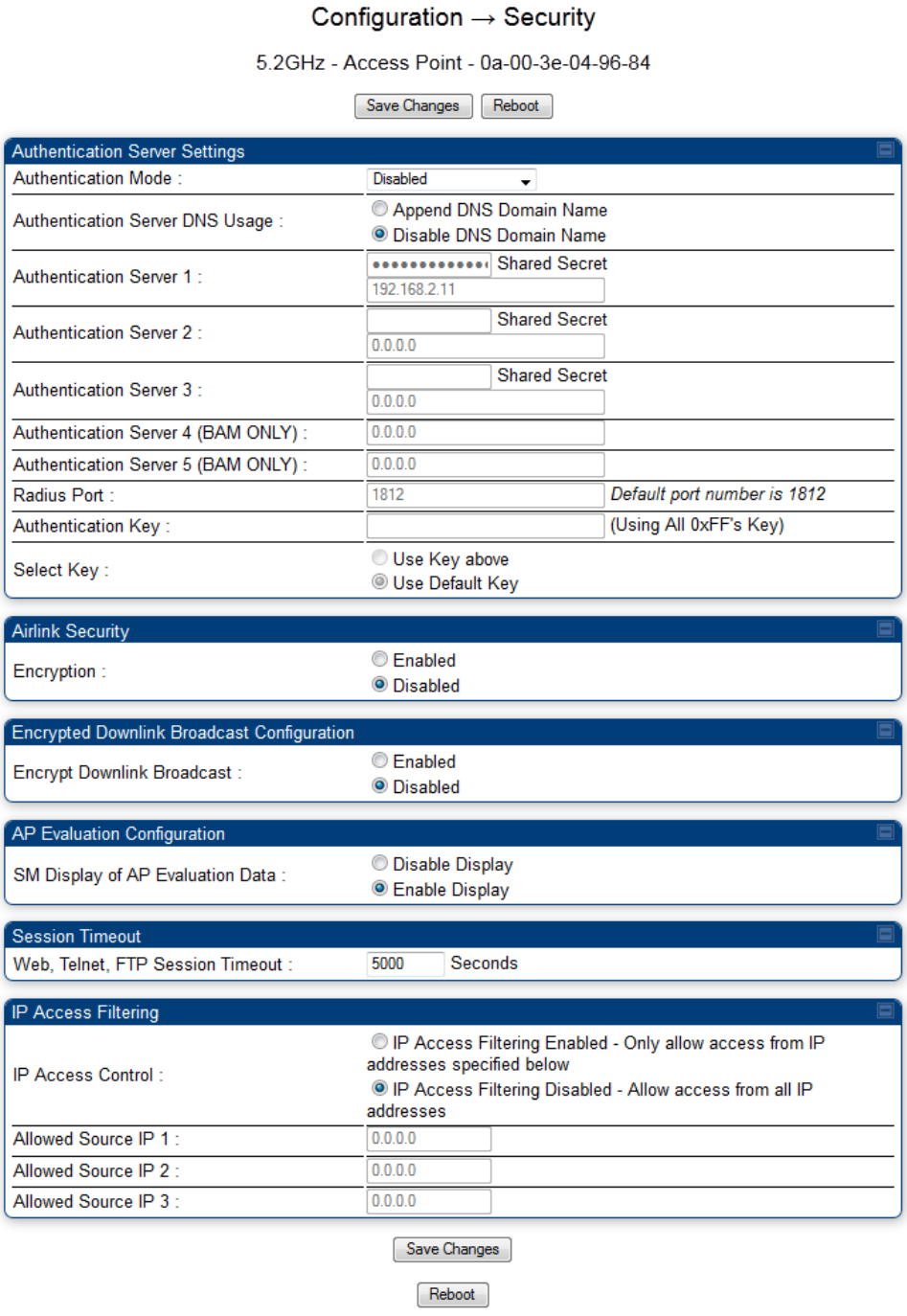


Figure 80: Security tab of AP, example

In the Security tab of the AP, you may set the following parameters.

Authentication Mode

If the AP has authentication capability, then you can use this field to select from among the following authentication modes:

- **Disabled**—the AP requires no SMs to authenticate.
- **Authentication Server** —the AP requires any SM that attempts registration to be authenticated in BAM or Prizm before registration.
- **AP PreShared Key** - The AP acts as the authentication server to its SMs and will make use of a user-configurable pre-shared authentication key. The operator enters this key on both the AP and all SMs desired to register to that AP. There is also an option of leaving the AP and SMs at their default setting of using the "Default Key". Due to the nature of the authentication operation, if you want to set a specific authentication key, then you MUST configure the key on all of the SMs and reboot them BEFORE enabling the key and option on the AP. Otherwise, if you configure the AP first, none of the SMs will be able to register.
- **RADIUS AAA** – the AP requires any SM that attempts registration to be authenticated via RADIUS

If the AP *does not* have authentication capability, then this parameter displays **Authentication Not Available**.

Authentication Server DNS Usage

The management DNS domain name may be toggled such that the name of the authentication server only needs to be specified and the DNS domain name is automatically appended to that name.

Authentication Server *1 to 5*

If either BAM or the BAM subsystem in Prizm is implemented and the AP has authentication capability, enter the IP address of one or more BAM servers that perform authentication for SMs registered to this AP.

Radius Port

This field allows the operator to configure a custom port for RADIUS server communication. The default value is 1812.

Authentication Key

The authentication key is a 32-character hexadecimal string used when **Authentication Mode** is set to **AP PreShared Key**. By default, this key is set to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF.

Select Key

This option allows operators to choose which authentication key is used:

- **Use Key above** means that the key specified in **Authentication Key** is used for authentication
- **Use Default Key** means that a default key (based off of the SM's MAC address) will be used for authentication

Encryption

Specify the type of air link security to apply to this AP:

- **Encryption Disabled** provides no encryption on the air link. This is the default mode.
- **Encryption Enabled** provides encryption, using a factory-programmed secret key that is unique for each module.

Encrypt Downlink Broadcast

When **Encryption Enabled** is selected in the **Airlink Security** parameter (described above) and **Enable** is selected in the Encrypt Downlink Broadcast parameter, the AP encrypts downlink broadcast packets as

- DES where the AP is DES capable.
- AES where the AP is AES capable.

For more information about the Encrypt Downlink Broadcast feature, see Encrypting Downlink Broadcasts on Page 438.

SM Display of AP Evaluation Data

You can use this field to suppress the display of data about this AP on the AP Evaluation tab of the Tools page in all SMs that register.

Web, Telnet, FTP Session Timeout

Enter the expiry in seconds for remote management sessions via HTTP, telnet, or ftp access to the AP.

IP Access Control

You can permit access to the AP from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address, including access and management by Prizm.

Allowed Source IP *1 to 3*

If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the AP from any IP address. You may populate as many as all three.

If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.

The Security tab of the AP also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

VLAN Tab of the AP

An example of the AP VLAN tab is displayed in Figure 81.

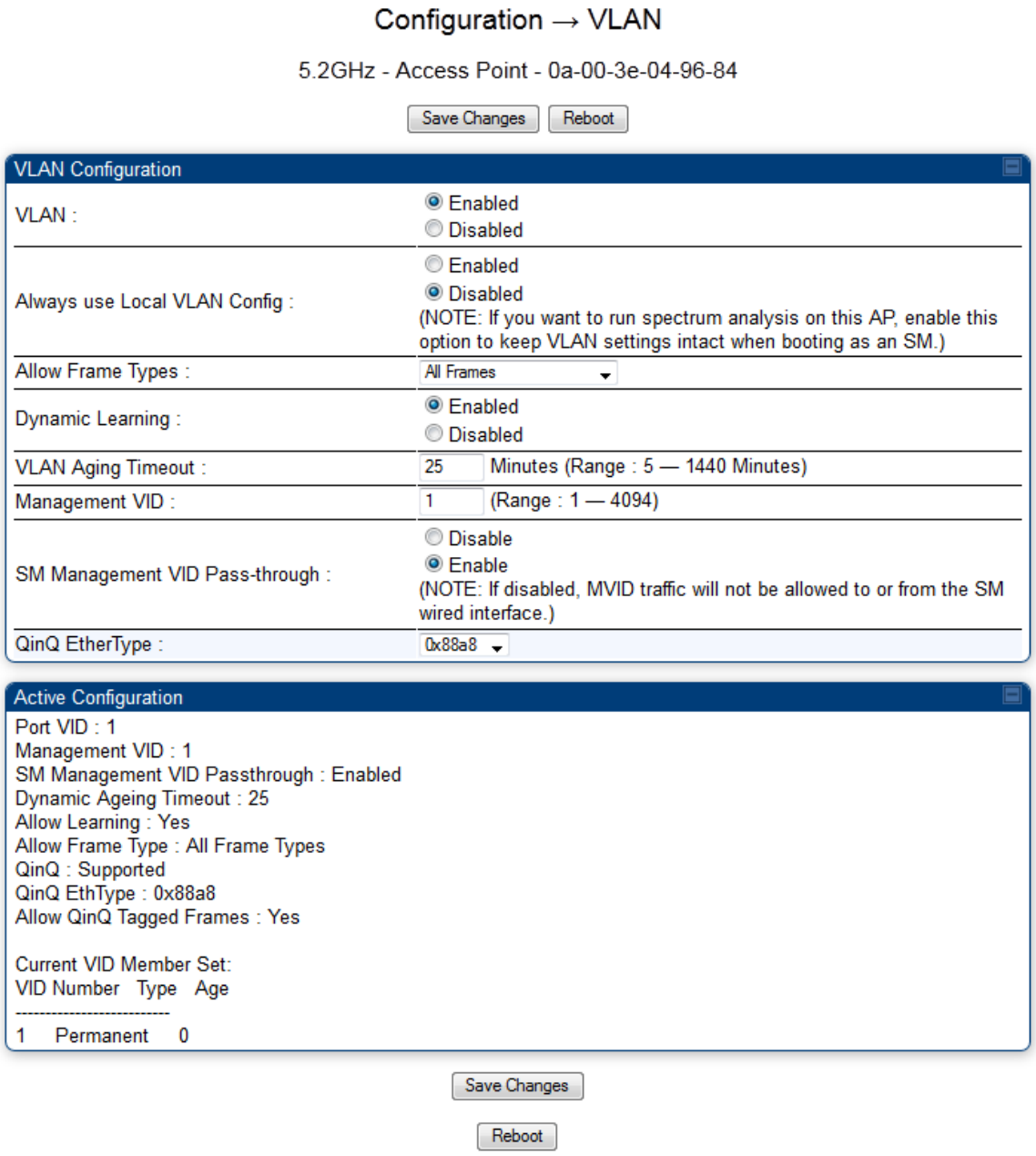


Figure 81: VLAN tab of AP, example

In the VLAN tab of the AP, you may set the following parameters.

VLAN

Specify whether VLAN functionality for the AP and all linked SMs should (Enabled) or should not (Disabled) be allowed. The default value is Disabled.

Always use Local VLAN Config

Enable this option before you reboot this AP as an SM to use it to perform spectrum analysis. After the spectrum analysis is completed and before you reboot this module as an AP, disable this option.

Allow Frame Types

Select the type of arriving frames that the AP should tag, using the VID that is stored in the **Untagged Ingress VID** parameter. The default value is **All Frames**.

Dynamic Learning

Specify whether the AP should (**Enabled**) or should not (**Disabled**) add the VLAN IDs (VIDs) of upstream frames to the VID table. (The AP passes frames with VIDs that are stored in the table both upstream and downstream.) The default value is **Enabled**.

VLAN Aging Timeout

Specify how long the AP should keep dynamically learned VIDs. The range of values is 5 to 1440 (minutes). The default value is **25** (minutes).

NOTE:
VIDs that you enter for the **Management VID** and **VLAN Membership** parameters do not time out.

Management VID

Enter the VID that the operator wishes to use to communicate with the module manager. The range of values is 1 to 4095. The default value is **1**.

SM Management VID Pass-through

Specify whether to allow the SM (**Enable**) or the AP (**Disable**) to control the VLAN settings of the SM. The default value is **Enable**.

CAUTION!

Do not set this parameter to **Enable** where both

- a BAM release earlier than 2.1 is implemented.
- the **Configuration Source** parameter in the AP is set to **BAM**.

This combination causes the SMs to become unmanageable, until you gain direct access with an override plug and remove this combination from the AP configuration.

QinQ EtherType

This parameter is the outer S-VLAN Ethertype that may be configured to interoperate with other networks that use a different Ethertype than the default.

Active Configuration

When VLAN is enabled in the AP, the Active Configuration block provides the following details as read-only information in this tab. In the Cambium fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

Port VID

This is the VID that the AP will use for tagging frames of the type specified by **Allow Frame Types**.

Management VID

This is the value of the parameter of the same name, configured above.

SM Management VID Pass-Through

This is the value of the parameter of the same name, configured above.

Dynamic Ageing Timeout

This is the value of the **VLAN Aging Timeout** parameter configured above.

Allow Learning

Yes is displayed if the value of the **Dynamic Learning** parameter above is **Enabled**. No is displayed if the value of **Dynamic Learning** is **Disabled**.

Allow Frame Type

This displays the selection that was made from the drop-down list at the **Allow Frame Types** parameter above.

Current VID Member Set, VID Number

This column lists the ID numbers of the VLANs in which this module is a member, whether through assignment or through dynamic learning.

Current VID Member Set, Type

For each VID number in the first column, the entry in this column correlates the way in which the module became and continues to be a member:

- **Permanent**—This indicates that the module was assigned the VID number through direct configuration by the operator.
- **Dynamic**—This indicates that the module adopted the VID number through enabled dynamic learning, when a tagged packet from an SM behind it in the network, or from a customer equipment that is behind the SM in this case, was read.

Current VID Member Set, Age

For each VID number in the first column of the table, the entry in this column reflects whether or when the VID number will time out:

- for **Permanent** type—the number will never time out, and this is indicated by the digit 0.
- for **Dynamic** type—the **Age** reflects what is configured in the **VLAN Aging Timeout** parameter in the Configuration => VLAN tab of the AP or reflects a fewer number of minutes that represents the difference between what was configured and what has elapsed since the VID was learned. Each minute, the Age decreases by one ucntil, at zero, the AP deletes the learned VID, but can it again from packets sent by elements that are beneath it in the network.

IMPORTANT!

Values in this Active Configuration block can differ from attempted values in configurations:

- A VLAN profile administered by the BAM subsystem in Prizm is capable of overriding any configured VLAN value, if the **Configuration Source** parameter in the AP is set to **Authentication Server**.
- The AP itself can override the value that the SM has configured for **SM Management VID Pass-Through**.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

VLAN Membership Tab of the AP

An example of the VLAN Membership tab of the AP is displayed in Figure 82.

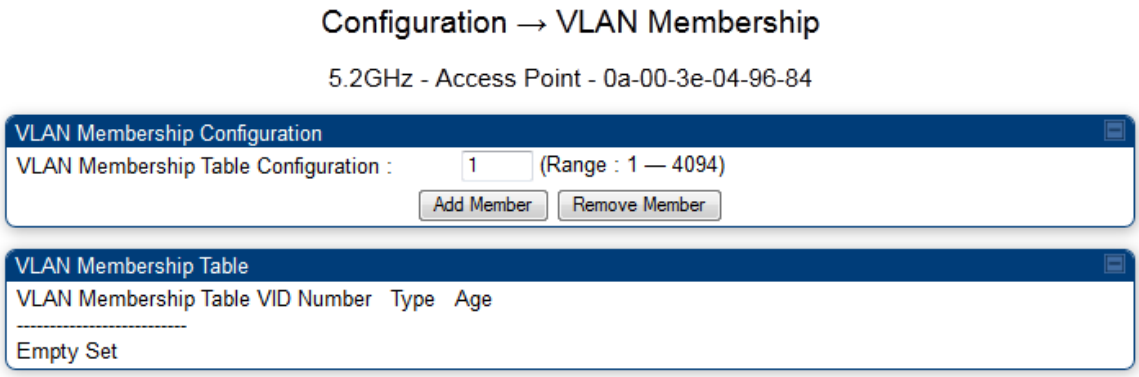


Figure 82: VLAN Membership tab of AP, example

You may set the VLAN Membership tab parameter as follows.

VLAN Membership Table Configuration

For each VLAN in which you want the AP to be a member, enter the VLAN ID and then click the **Add Member** button. Similarly, for any VLAN in which you want the AP to no longer be a member, enter the VLAN ID and then click the **Remove Member** button.

Diffserv Tab of the AP

An example of the Diffserv tab of the AP is displayed in Figure 83.

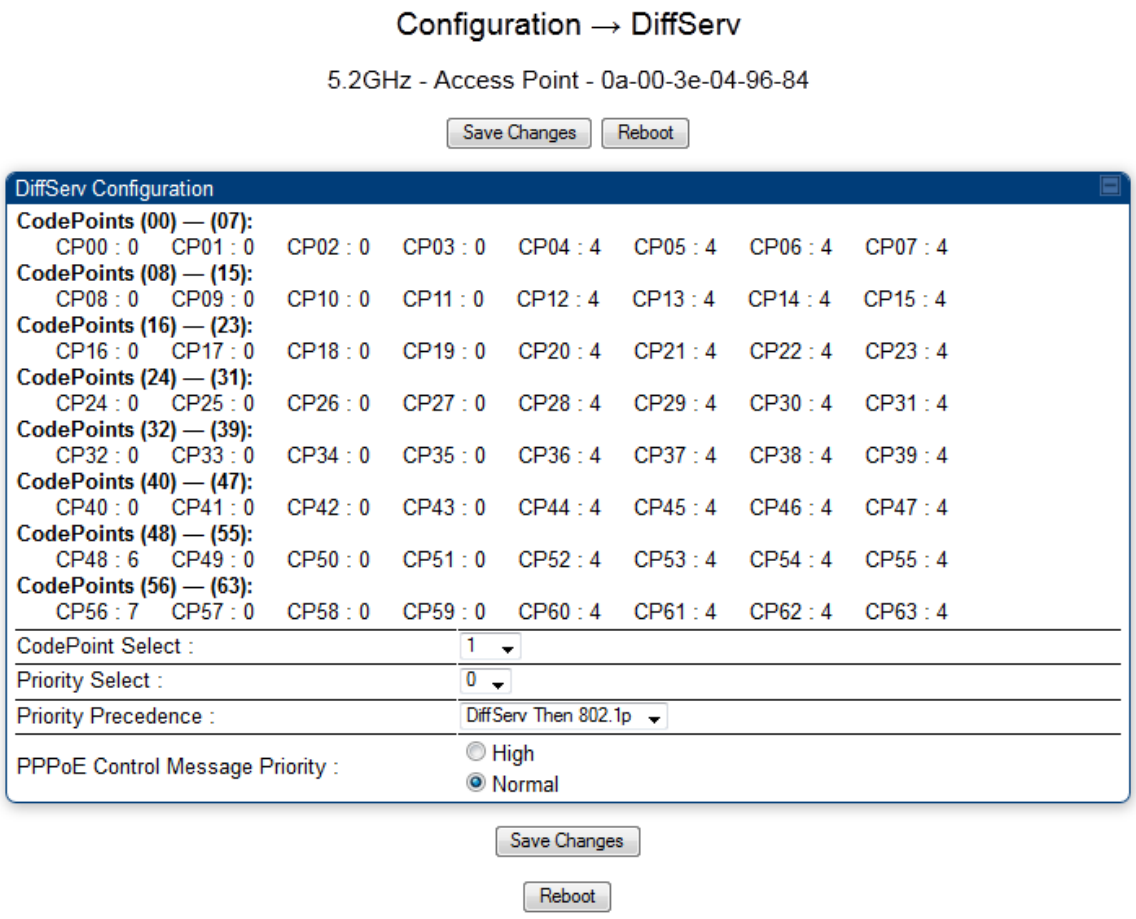

Configuration → DiffServ
5.2GHz - Access Point - 0a-00-3e-04-96-84
Save Changes
Reboot
DiffServ Configuration
CodePoints (00) — (07):
CP00 : 0 CP01 : 0 CP02 : 0 CP03 : 0 CP04 : 4 CP05 : 4 CP06 : 4 CP07 : 4
CodePoints (08) — (15):
CP08 : 0 CP09 : 0 CP10 : 0 CP11 : 0 CP12 : 4 CP13 : 4 CP14 : 4 CP15 : 4
CodePoints (16) — (23):
CP16 : 0 CP17 : 0 CP18 : 0 CP19 : 0 CP20 : 4 CP21 : 4 CP22 : 4 CP23 : 4
CodePoints (24) — (31):
CP24 : 0 CP25 : 0 CP26 : 0 CP27 : 0 CP28 : 4 CP29 : 4 CP30 : 4 CP31 : 4
CodePoints (32) — (39):
CP32 : 0 CP33 : 0 CP34 : 0 CP35 : 0 CP36 : 4 CP37 : 4 CP38 : 4 CP39 : 4
CodePoints (40) — (47):
CP40 : 0 CP41 : 0 CP42 : 0 CP43 : 0 CP44 : 4 CP45 : 4 CP46 : 4 CP47 : 4
CodePoints (48) — (55):
CP48 : 6 CP49 : 0 CP50 : 0 CP51 : 0 CP52 : 4 CP53 : 4 CP54 : 4 CP55 : 4
CodePoints (56) — (63):
CP56 : 7 CP57 : 0 CP58 : 0 CP59 : 0 CP60 : 4 CP61 : 4 CP62 : 4 CP63 : 4
CodePoint Select :
1
Priority Select :
0
Priority Precedence :
DiffServ Then 802.1p
PPPoE Control Message Priority :
High
Normal
Save Changes
Reboot

Figure 83: Diffserv tab of AP, example

You may set the following Diffserv tab parameters.

CodePoint 1 through CodePoint 47

CodePoint 49 through CodePoint 55

CodePoint 57 through CodePoint 63

The default priority value for each settable CodePoint is shown in Figure 118. Priorities of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities.

Consistent with RFC 2474

- **CodePoint 0** is predefined to a fixed priority value of **0** (low-priority channel).
- **CodePoint 48** is predefined to a fixed priority value of **6** (high-priority channel).
- **CodePoint 56** is predefined to a fixed priority value of **7** (high-priority channel).

You cannot change any of these three fixed priority values. Among the settable parameters, the priority values (and therefore the handling of packets in the high- or low-priority channel) are set in the AP for all downlinks within the sector and in the SM for each uplink. See DSCP Field on Page 87.

CodePoint Select

This represents the CodePoint Selection to be modified via Priority Select

Priority Select

The priority setting input for the CodePoint selected in CodePoint Select

Priority Precedence

Allows operator to decide if 802.1p or DiffServ priority bits should be used first when making priority decisions.

PPPoE Control Message Priorty

Operators may configure the AP to utilize the high priority channel for PPPoE control messages. Configuring the AP in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the AP.

The Diffserv tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented

Protocol Filtering Tab of the AP

An example of the Protocol Filtering tab in an AP is displayed in Figure 98.

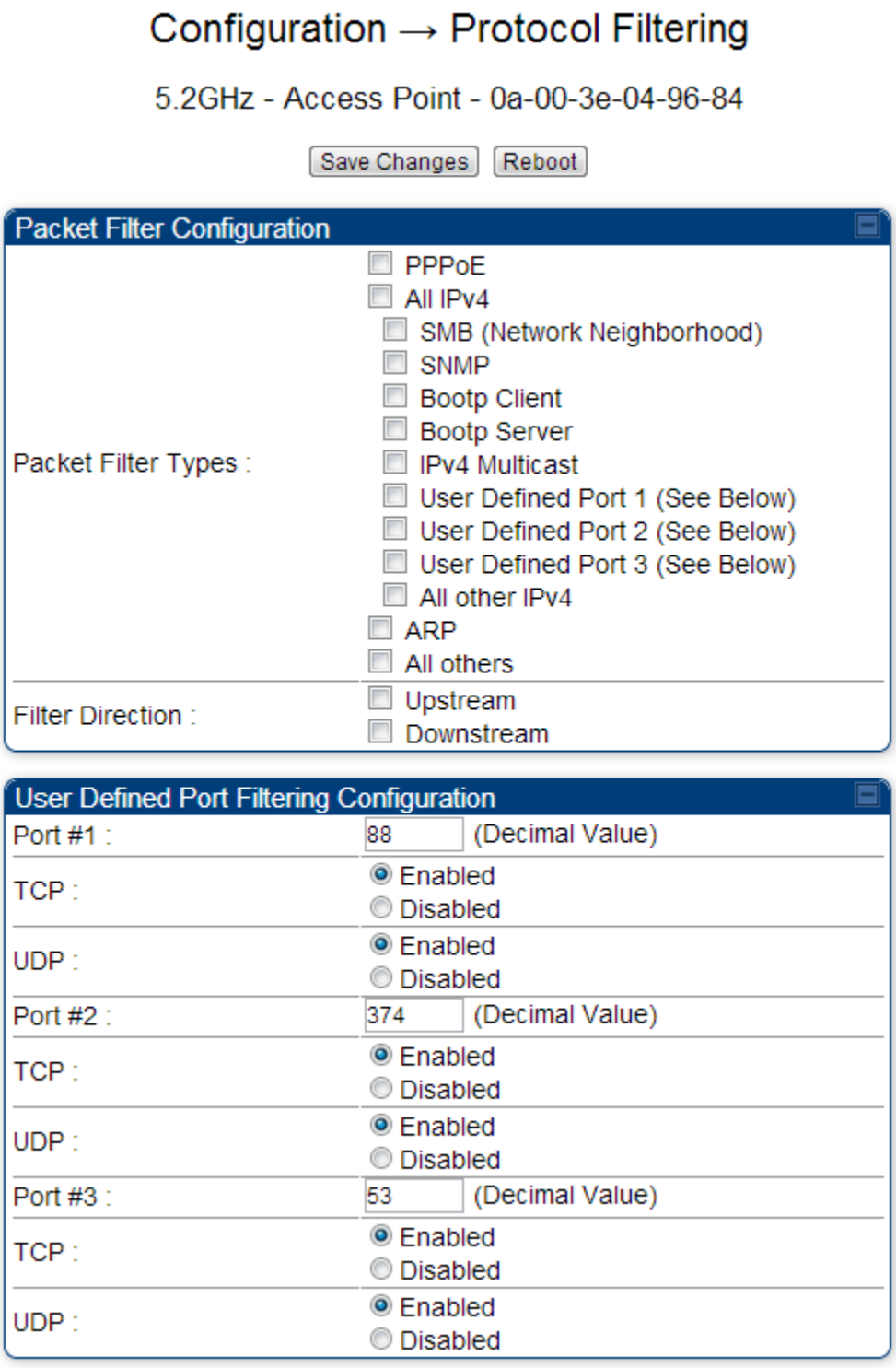


Figure 84: Protocol Filtering tab of AP, example

In the Protocol Filtering tab of the AP, you may set the following parameters.

Packet Filter Types

For any box selected, the Protocol and Port Filtering feature blocks the associated protocol type. Examples are provided in Protocol and Port Filtering with NAT Disabled on Page 436.

To filter packets in any of the user-defined ports, you must do all of the following:

- Check the box for User Defined Port *n* (See Below) in the Packet Filter Types section of this tab.
- In the User Defined Port Filtering Configuration section of this tab, both
  - provide a port number at **Port #*n***.
  - check **TCP**, **UDP**, or both.

If the **DHCP state** parameter is set to **Enabled** in the Configuration => IP tab of the AP, *do not* check the **Bootp Client** option for **Packet Filter Types** in its Protocol Filtering tab, because doing so would block the DHCP request. (Filters apply to all packets that leave the AP via its RF interface, including those that the AP itself generates.) If you want to keep DHCP enabled and avoid the blocking scenario, select the **Bootp Server** option instead. This will result in responses being appropriately filtered and discarded.

Filter Direction

Select which direction of traffic should be filtered – Upstream (uplink) or Downstream (downlink).

User Defined Port Filtering Configuration

You can specify ports for which to block access. For more information, see Filtering Protocols and Ports on Page 435.

Unit Settings Tab of the AP

An example of the Unit Settings tab of the AP is shown in Figure 85.

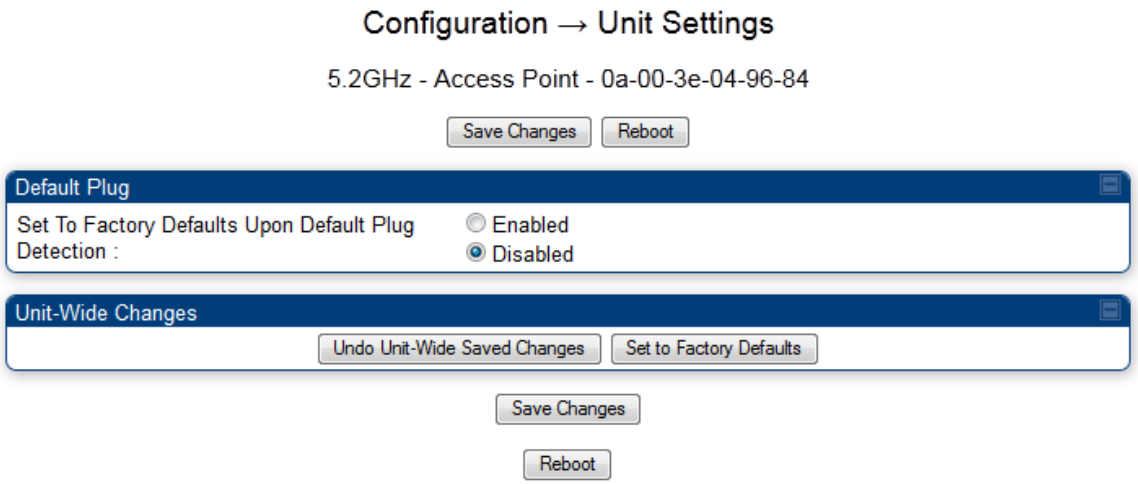


Figure 85: Unit Settings tab of AP, example

The Unit Settings tab of the AP contains an option for how the AP should react when it detects a connected override plug. You may set this option as follows.

Set to Factory Defaults Upon Default Plug Detection

If **Enabled** is checked, then an override/default plug functions as a default plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all parameter values are reset to defaults. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *cannot* see or learn the settings that were previously configured in it. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the default values for any that were not.

If **Disabled** is checked, then an override/default plug functions as an override plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all previously configured parameter values remain and are displayed. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *can* see and learn the settings. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the previous values for any that were not.

See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 433.

The Unit Settings tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Undo Unit-Wide Saved Changes

When you click this button, any changes that you made in any tab but did not commit by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all tabs* are reset to the factory settings.

Configuring an SM for the Destination

If an ADMINISTRATOR-level password has been set in the SM, you must log into the module before you can configure its parameters. See Managing Module Access by Passwords on Page 430.

General Tab of the SM

An example of a General tab in the SM is displayed in Figure 86.

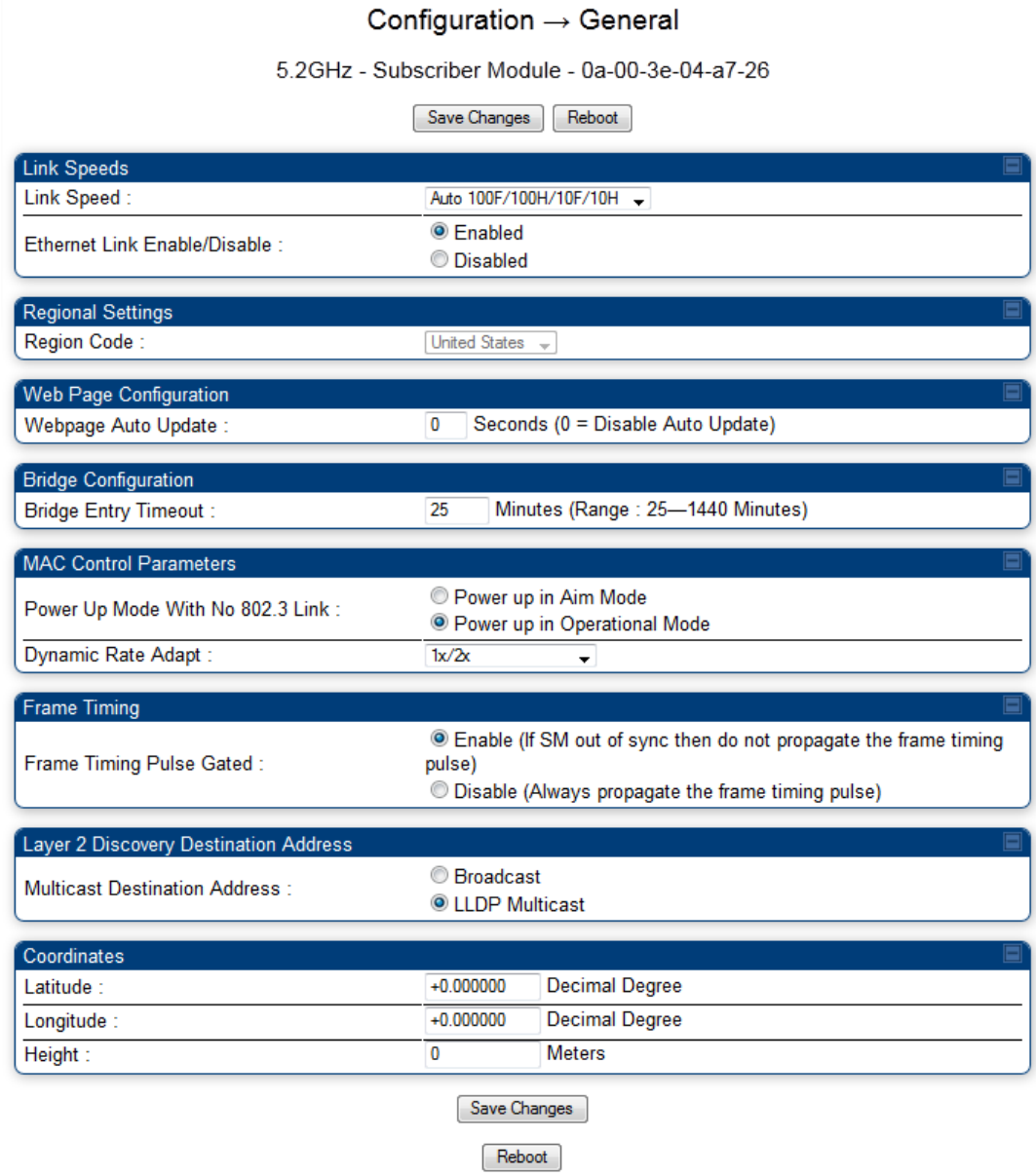


Figure 86: General tab of SM, example

In the General tab of the SM, you may set the following parameters.

Link Speed

From the drop-down list of options, select the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all APs, BHs, and SMs in the operator network.

Ethernet Link Enable/Disable

Specify whether to enable or disable Ethernet/802.3 connectivity on the wired port of the SM. This parameter has no effect on the wireless link. When you select **Enable**, this feature allows traffic on the Ethernet/802.3 port. This is the factory default state of the port. When you select **Disable**, this feature prevents traffic on the port. Typical cases of when you may want to select **Disable** include:

- The subscriber is delinquent with payment(s).
- You suspect that the subscriber is sending or flooding undesired broadcast packets into the network, such as when
  - a virus is present in the subscriber's computing device.
  - the subscriber's home router is improperly configured.

Region Code

This parameter allows you to set the region in which the radio will operate. When the appropriate region has been set, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard. For further information on DFS, see Radar Signature Detection and Shutdown on Page 127.

The slave radio automatically inherits the DFS type of the master. This behavior ignores the value of the **Region Code** parameter in the slave, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), this parameter should always be set to the value that corresponds to the local region.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

Bridge Entry Timeout

Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. Timeout occurs when the AP encounters no activity with the SM (whose MAC address is the bridge entry) within the interval that this parameter specifies. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.

This parameter governs the timeout interval, even if a router in the system has a longer timeout interval. The default value of this field is 25 minutes.

CAUTION!
An inappropriately low **Bridge Entry Timeout** setting may lead to temporary loss of communication with some end users.

SM Power Up Mode With No 802.3 Link

This parameter is present in only PMP 100 Series SMs. Specify the default mode in which this SM will power up when the SM senses no Ethernet link. Select either

- **Power Up in Aim Mode**—the SM boots in an aiming mode. When the SM senses an Ethernet link, this parameter is automatically reset to Power Up in Operational Mode. When the module senses no Ethernet link within 15 minutes after power up, the SM carrier shuts off.
- **Power Up in Operational Mode**—the SM boots in Operational mode. The module attempts registration. This is the default selection.

Dynamic Rate Adapt (PMP 100 Series)

This parameter is present in only PMP 100 Series (FSK) SMs. Whatever value that you set in this parameter is overridden by a lock-down to 1X operation, if that is configured in the AP. In some cases, disabling this parameter facilitates aiming. Be aware that a lock-down to 1X in the AP locks down the uplink and downlink between the AP and all SMs in its sector, and thus would affect traffic and performance across the entire sector. Hence, a temporary lock-down for aiming is better done in the individual SM. See 2X Operation on Page 89.

Dynamic Rate Adapt (PMP 400 Series)

This parameter is present in only PMP 400 Series (OFDM) SMs. Whatever value that you set in this parameter is overridden by a lock-down to 1X or 2X operation, if that is configured in the AP. As with the **2X Rate** parameter in a PMP 100 Series SM, a temporary lock-down to facilitate aiming may be helpful. Be aware that a lock-down to 1X or 2X in the AP locks down the uplink and downlink between the AP and all SMs in its sector, and thus would affect traffic and performance across the entire sector. Hence, a temporary lock-down for aiming is better done in the individual SM. See 2X Operation on Page 89 and 3X Operation on Page 92.

Frame Timing Pulse Gated

If this SM extends the sync pulse to a BH master or an AP, select either

- **Enable**—If this SM loses sync from the AP, then *do not* propagate a sync pulse to the BH timing master or other AP. This setting prevents interference in the event that the SM loses sync.

- **Disable**—If this SM loses sync from the AP, then propagate the sync pulse to the BH timing master or other AP.

See Wiring to Extend Network Sync on Page 426.

The General tab also contains the following buttons.

Multicast Destination Address

Using Link Layer Discovery Protocol (LLDP), a module exchanges multicast addresses with the device to which it is wired on the Ethernet interface. Although some switches (CMMmicro, for example) do not pass LLDP addresses upward in the network, a radio can pass it as the value of the **Multicast Destination Address** parameter value in the connected device that has it populated.

In this way, an SM can report to Prizm, for example, the multicast address of a connected remote AP, and thus allow Prizm to discover that AP. To allow this, set the message mode in the remote AP to **LLDP Multicast**. Set this parameter in the SM to **Broadcast**. The SM will pass this address in broadcast mode, and the CMMmicro will pass the address upward in the network, since it does not discard addresses that it receives in broadcast mode.

Where the AP is not behind another device, the **Broadcast** mode will allow discovery of the AP.

Coordinates

Physical radio location data may be configured via the **Latitude**, **Longitude**, and **Height** fields.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

NAT and IP Tabs of the SM with NAT Disabled

An example of the NAT tab in an SM with NAT disabled is displayed in Figure 87.

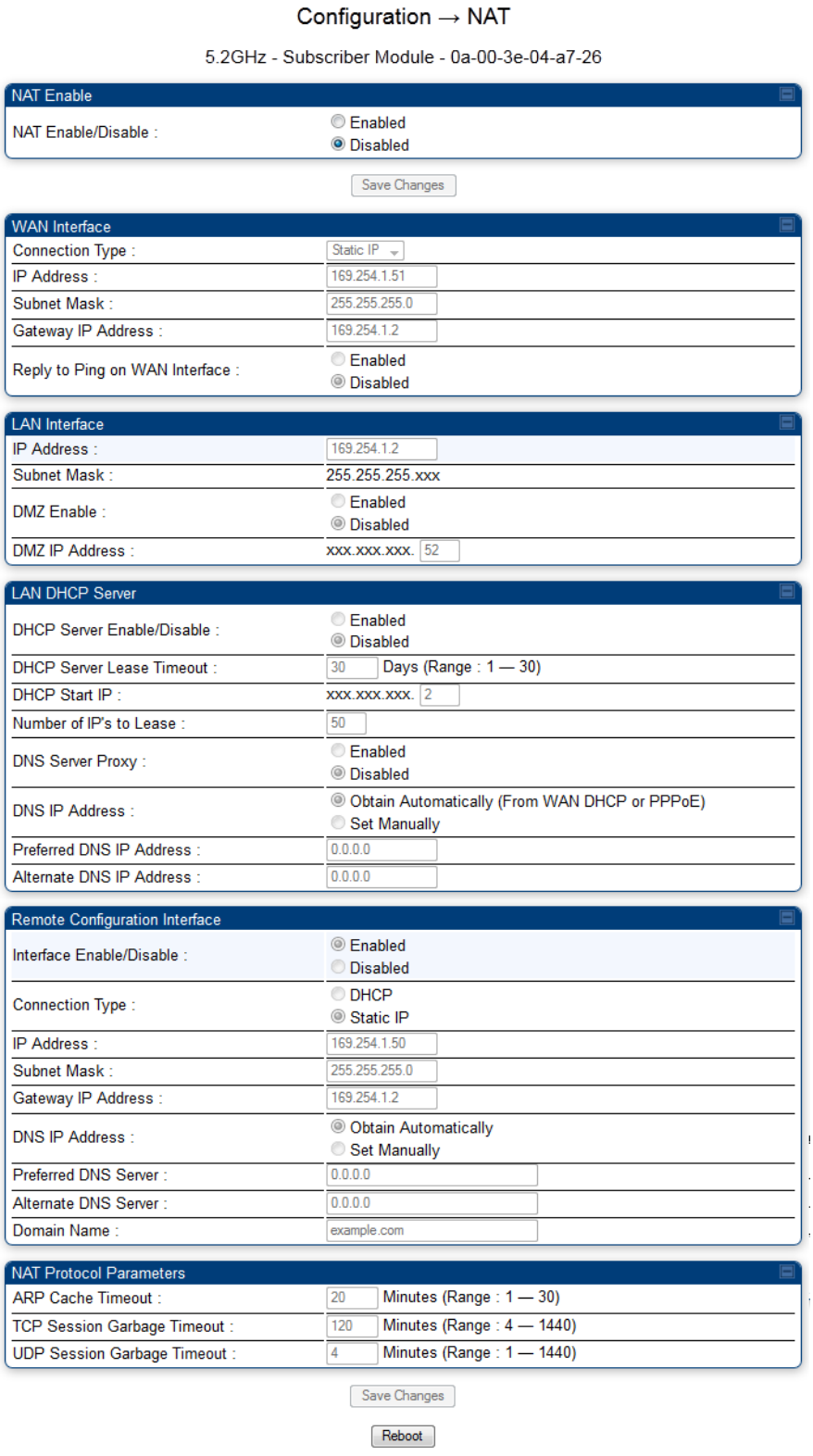


Figure 87: NAT tab of SM with NAT disabled, example

This implementation is illustrated in Figure 48 on Page 159. In the NAT tab of an SM with NAT disabled, you may set the following parameters.

NAT Enable/Disable

This parameter enables or disabled the Network Address Translation (NAT) feature for the SM. NAT isolates devices connected to the Ethernet/wired side of an SM from being seen directly from the wireless side of the SM. With NAT enabled, the SM has an IP address for transport traffic separate from its address for management, terminates transport traffic, and allows you to assign a range of IP addresses to devices that are connected to the Ethernet/wired side of the SM. For further information, see Network Address Translation (NAT) on Page 158 and NAT and IP Tabs of the SM with NAT Enabled on Page 287.

When NAT is enabled, VLANs are not supported on the wired side of that SM. You can enable NAT in SMs within a sector where VLAN is enabled in the AP, but this may constrain network design.

WAN Interface, Connection Type

This parameter is not configurable when NAT is disabled.

WAN Interface, IP Address

This field displays the IP address for the SM. DHCP Server *will not* automatically assign this address when NAT is disabled.

WAN Interface, Subnet Mask

This field displays the subnet mask for the SM. DHCP Server *will not* automatically assign this address when NAT is disabled.

WAN Interface, Gateway IP Address

This field displays the gateway IP address for the SM. DHCP Server *will not* automatically assign this address when NAT is disabled.

WAN Interface, Reply to Ping on WAN Interface

This parameter is not configurable when NAT is disabled.

LAN Interface, IP Address

This parameter is not configurable when NAT is disabled.

LAN Interface, Subnet Mask

This parameter is not configurable when NAT is disabled.

LAN Interface, DMZ Enable

This parameter is not configurable when NAT is disabled.

LAN Interface, DMZ IP Address

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, DHCP Server Enable/Disable

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, DHCP Server Lease Timeout

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, DHCP Start IP

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, Number of IPs to Lease

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, DNS Server Proxy

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, DNS IP Address

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, Preferred DNS IP Address

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, Alternate DNS IP Address

This parameter is not configurable when NAT is disabled.

Remote Configuration Interface, Interface Enable/Disable

This parameter is not configurable when NAT is disabled.

Remote Configuration Interface, Connection Type

This parameter is not configurable when NAT is disabled.

Remote Configuration Interface, IP Address

This parameter is not configurable when NAT is disabled.

Remote Configuration Interface, Subnet Mask

This parameter is not configurable when NAT is disabled.

Remote Configuration Interface, Gateway IP Address

This parameter is not configurable when NAT is disabled.

Remote Configuration Interface, DNS IP Address

This parameter is not configurable when NAT is disabled

Remote Configuration Interface, Preferred DNS Server

This parameter is not configurable when NAT is disabled

Remote Configuration Interface, Alternate DNS SErver

This parameter is not configurable when NAT is disabled

Remote Configuration Interface, Domain Name

This parameter is not configurable when NAT is disabled

NAT Protocol Parameters, ARP Cache Timeout

If a router upstream has an ARP cache of longer duration (as some use 30 minutes), enter a value of longer duration than the router ARP cache. The default value of this field is 20 minutes.

NAT Protocol Parameters, TCP Session Garbage Timeout

Where a large network exists behind the SM, you can set this parameter to lower than the default value of 1440 minutes (24 hours). This action makes additional resources available for greater traffic than the default value accommodates.

NAT Protocol Parameters, UDP Session Garbage Timeout

You may adjust this parameter in the range of 1 to 1440 minutes, based on network performance. The default value of this parameter is 4 minutes.

The NAT tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

An example of the IP tab in an SM with NAT disabled is displayed in Figure 88.

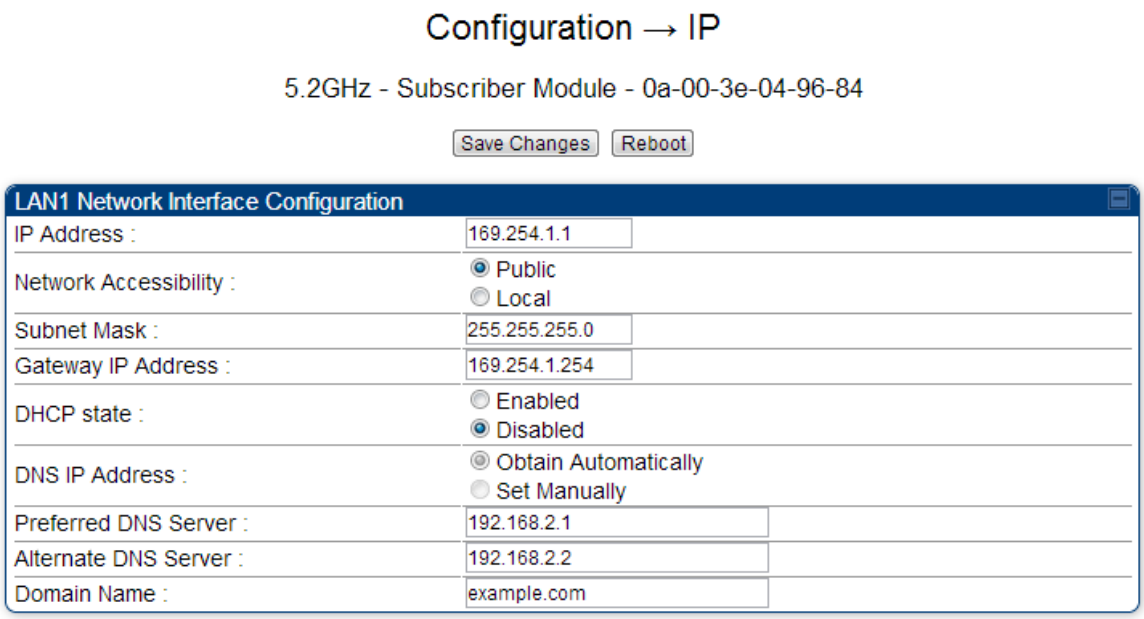


Figure 88: IP tab of SM with NAT disabled, example

This implementation is illustrated in Figure 48 on Page 159. In the IP tab of an SM with NAT disabled, you may set the following parameters.

LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to associate with the Ethernet connection on this SM. (The default IP address from the factory is 169.254.1.1.) If you set and then forget this parameter, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 433.

RECOMMENDATION:
Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN1 Network Interface Configuration, Network Accessibility

Specify whether the IP address of the SM should be visible to only a device connected to the SM by Ethernet (**Local**) or should be visible to the AP as well (**Public**).

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the SM to communicate on the network. The default subnet mask is 255.255.0.0. See Allocating Subnets on Page 164.

LAN1 Network Interface Configuration, Gateway IP Address

Enter the appropriate gateway for the SM to communicate with the network. The default gateway is 169.254.0.0.

LAN1 Network Interface Configuration, DHCP state

If you select **Enabled**, the DHCP server automatically assigns the IP configuration (IP address, subnet mask, and gateway IP address) and the values of those individual parameters (above) are not used. The setting of this DHCP state parameter is also viewable, but not settable, in the Network Interface tab of the Home page.

In this tab, DHCP State is settable only if the **Network Accessibility** parameter in the IP tab is set to **Public**. This parameter is also settable in the NAT tab of the Configuration web page, but only when NAT is enabled.

If the **DHCP state** parameter is set to **Enabled** in the Configuration => IP tab of the SM, *do not* check the **BootpClient** option for **Packet Filter Types** in its Protocol Filtering tab, because doing so would block the DHCP request. (Filters apply to all packets that leave the SM via its RF interface, including those that the SM itself generates.) If you want to keep DHCP enabled and avoid the blocking scenario, select the **Bootp Server** option instead. This will result in responses being appropriately filtered and discarded.

The IP tab also contains the following buttons.

LAN1 Network Interface Configuration, DNS IP Address

Canopy devices allow for configuration of a preferred and alternate DNS server IP address either automatically or manually. Devices must set DNS server IP address manually when DHCP is disabled for the management interface of the device. DNS servers may be configured automatically from the DHCP response when DHCP is enabled for the management interface of the device. Optionally devices may be configured to set the DNS server IP address manually when DHCP is enabled for the management interface. The default DNS IP addresses are 0.0.0.0 when configured manually.

LAN1 Network Interface Configuration, Preferred DNS Server

The first address used for DNS resolution.

LAN1 Network Interface Configuration, Alternate DNS Server

Upon failure to reach the Preferred DNS server, the Alternate DNS Server is used.

LAN1 Network Interface Configuration, Domain Name

The operator's management domain name may be configured for DNS. The domain name configuration can be used for configuration of the servers in the operator's network. The default domain name is example.com, and is only used if configured as such.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

NAT and IP Tabs of the SM with NAT Enabled

An example of the NAT tab in an SM with NAT enabled is displayed in Figure 89.

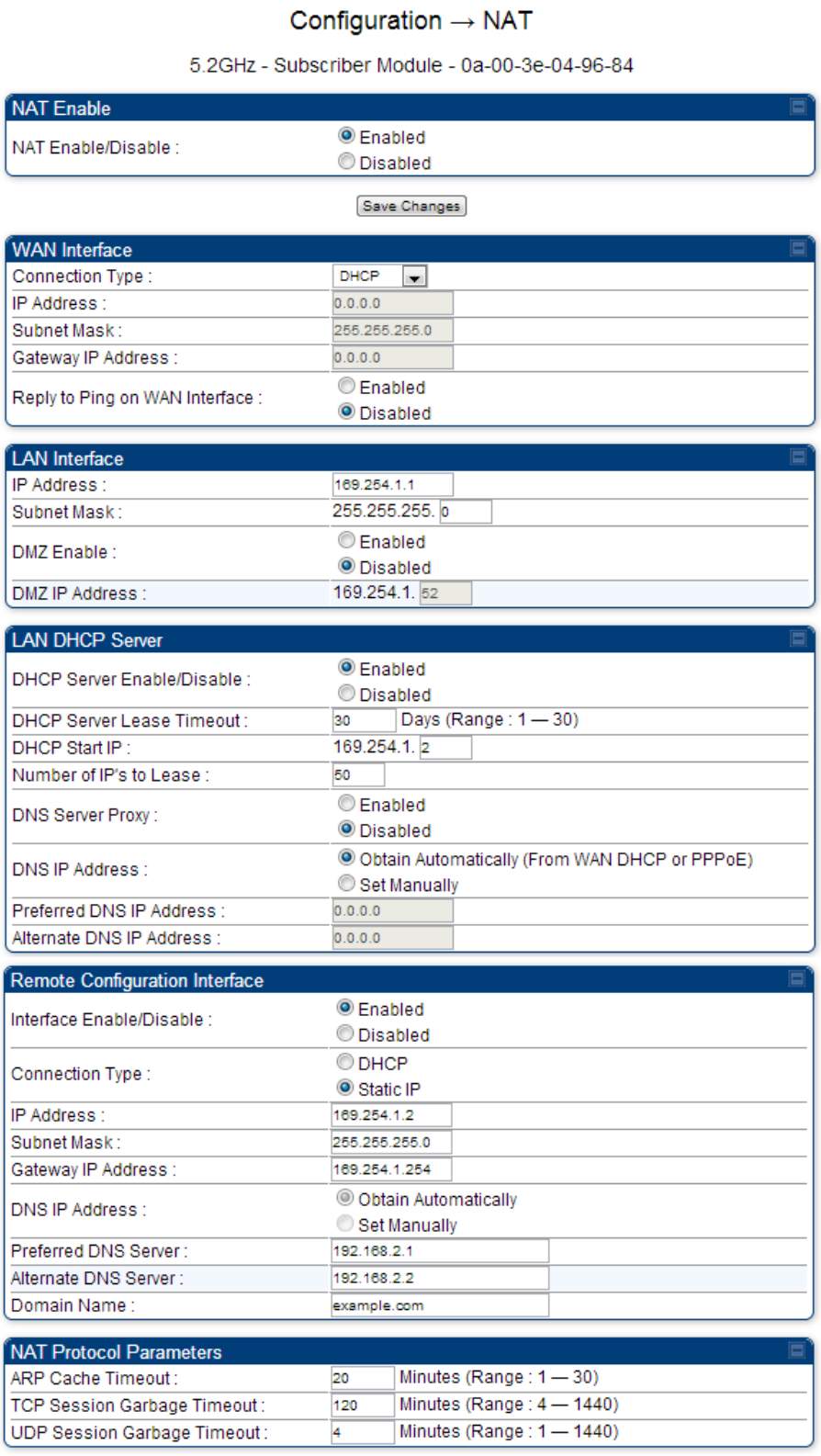


Figure 89: NAT tab of SM with NAT enabled, example

In the NAT tab of an SM with NAT enabled, you may set the following parameters.

NAT Enable/Disable

This parameter enables or disabled the Network Address Translation (NAT) feature for the SM. NAT isolates devices connected to the Ethernet/wired side of an SM from being seen directly from the wireless side of the SM. With NAT enabled, the SM has an IP address for transport traffic separate from its address for management, terminates transport traffic, and allows you to assign a range of IP addresses to devices that are connected to the Ethernet/wired side of the SM. For further information, see Network Address Translation (NAT) on Page 158 and NAT and IP Tabs of the SM with NAT Enabled on Page 287.

When NAT is enabled, VLANs are not supported on the wired side of that SM. You can enable NAT in SMs within a sector where VLAN is enabled in the AP, but this may constrain network design.

WAN Interface

The WAN interface is the RF-side address for transport traffic.

WAN Interface, Connection Type

This parameter may be set to

- **Static IP**—when this is the selection, the following three parameters (**IP Address**, **Subnet Mask**, and **Gateway IP Address**) must all be properly populated.
- **DHCP**—when this is the selection, the information from the DHCP server configures the interface.
- **PPPoE**—when this is the selection, the information from the PPPoE server configures the interface.

WAN Interface, IP Address

If **Static IP** is set as the **Connection Type** of the WAN interface, then this parameter configures the IP address of the SM for RF transport traffic.

WAN Interface, Subnet Mask

If **Static IP** is set as the **Connection Type** of the WAN interface, then this parameter configures the subnet mask of the SM for RF transport traffic.

WAN Interface, Gateway IP Address

If **Static IP** is set as the **Connection Type** of the WAN interface, then this parameter configures the gateway IP address for the SM for RF transport traffic.

WAN Interface, Reply to Ping on WAN Interface

By default, the radio interface *does not* respond to pings. If you use a management system (such as Prizm or WM) that will occasionally ping the SM, set this parameter to **Enabled**.

LAN Interface

The LAN interface is both the management access through the Ethernet port and the Ethernet-side address for transport traffic. When NAT is enabled, this interface is redundantly shown as the **NAT Network Interface Configuration** on the IP tab of the Configuration web page in the SM.

LAN Interface, IP Address

Assign an IP address for SM management through Ethernet access to the SM. This address becomes the base for the range of DHCP-assigned addresses.

LAN Interface, Subnet Mask

Assign a subnet mask of 255.255.255.0 or a more restrictive subnet mask. Set only the last byte of this subnet mask. Each of the first three bytes is permanently set to 255.

LAN Interface, DMZ Enable

Either enable or disable DMZ for this SM. See DMZ on Page 159.

LAN Interface, DMZ IP Address

If you enable DMZ in the parameter above, set the last byte of the DMZ host IP address to use for this SM when DMZ is enabled. Only one such address is allowed. The first three bytes are identical to those of the NAT private IP address. Ensure that the device that should receive network traffic behind this SM is assigned this address. The system provides a warning if you enter an address within the range that DHCP can assign.

LAN DHCP Server

This is the server (in the SM) that provides an IP address to the device connected to the Ethernet port of the SM.

LAN DHCP Server, DHCP Server Enable/Disable

Select either

- Enabled to
  - allow this SM to assign IP addresses, subnet masks, and gateway IP addresses to attached devices.
  - assign a start address for DHCP.
  - designate how many IP addresses may be temporarily used (leased).

- **Disabled** to disallow the SM to assign addresses to attached devices.

The implementation of NAT with DHCP server is illustrated in Figure 51 on Page 37.
The implementation of NAT with DHCP client (**DHCP** selected as the **Connection Type** of the WAN interface) and DHCP server is illustrated in Figure 49 on Page 160. The implementation of NAT without DHCP is illustrated in Figure 52 on Page 163.

LAN DHCP Server, DHCP Server Lease Timeout

Based on network performance, enter the number of days between when the DHCP server assigns an IP address and when that address expires. The range of values for this parameter is 1 to 30 days. The default value is 30 days.

LAN DHCP Server, DHCP Start IP

If you will be enabling DHCP Server below, set the last byte of the starting IP address that the DHCP server will assign. The first three bytes are identical to those of the NAT private IP address.

LAN DHCP Server, Number of IPs to Lease

Enter how many IP addresses the DHCP server is allowed to assign. The default value is 50 addresses.

LAN DHCP Server, DNS Server Proxy

This parameter enables or disables advertisement of the SM as the DNS server. On initial boot up of an SM with the NAT WAN interface configured as DHCP or PPPoE, the SM module will not immediately have DNS information. With **DNS Server Proxy** disabled, the clients will renew their lease about every minute until the SM has the DNS information to give out. At this point the SM will go to the full configured lease time period which is 30 days by default. With **DNS Server Proxy** enabled, the SM will give out full term leases with its NAT LAN IP as the DNS server.

LAN DHCP Server, DNS IP Address

Select either

- **Obtain Automatically** to allow the system to set the IP address of the DNS server.
- **Set Manually** to enable yourself to set both a preferred and an alternate DNS IP address.

LAN DHCP Server, Preferred DNS IP Address

Enter the preferred DNS IP address to use when the **DNS IP Address** parameter is set to **Set Manually**.

LAN DHCP Server, Alternate DNS IP Address

Enter the DNS IP address to use when the **DNS IP Address** parameter is set to **Set Manually** and no response is received from the preferred DNS IP address.

Remote Configuration Interface, Interface Enable/Disable

If you want over-the-air management capability for the SM, select **Enabled**. If you want to limit management of the SM to its Ethernet interface, select **Disabled**.

Remote Configuration Interface

The Remote Configuration interface is the RF-side address for management by an EMS or NMS (Prizm or WM, for example).

Remote Configuration Interface, Interface Enable/Disable

When this interface is **Disabled**, the SM is not directly accessible by IP address, and management access is only through either

- the LAN (Ethernet) interface
- a link from an AP web page into the WAN (RF-side) interface.

When this interface is **Enabled**, you can configure management access through either

- a **Static IP** address
- an IP address that **DHCP** provides for the WAN interface.

Remote Configuration Interface, Connection Type

This parameter may be set to

- **Static IP**—when this is the selection, the following three parameters (**IP Address**, **Subnet Mask**, and **Gateway IP Address**) must all be properly populated.
- **DHCP**—when this is the selection, the information from the DHCP server configures the interface.

Remote Configuration Interface, IP Address

If **Static IP** is set as the **Connection Type** of the WAN interface, then this parameter configures the IP address of the SM for RF management traffic.

Remote Configuration Interface, Subnet Mask

If **Static IP** is set as the **Connection Type** of the WAN interface, then this parameter configures the subnet mask of the SM for RF management traffic.

Remote Configuration Interface, Gateway IP Address

If **Static IP** is set as the **Connection Type** of the WAN interface, then this parameter configures the gateway IP address for the SM for RF management traffic.

RECOMMENDATION:
Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

NAT Protocol Parameters, ARP Cache Timeout

If a router upstream has an ARP cache of longer duration (as some use 30 minutes), enter a value of longer duration than the router ARP cache. The default value of this field is 20 minutes.

NAT Protocol Parameters, TCP Session Garbage Timeout

Where a large network exists behind the SM, you can set this parameter to lower than the default value of 1440 minutes (24 hours). This action makes additional resources available for greater traffic than the default value accommodates. The default value of this parameter is 120 minutes.

NAT Protocol Parameters, UDP Session Garbage Timeout

You may adjust this parameter in the range of 1 to 1440 minutes, based on network performance. The default value of this parameter is 4 minutes.

The NAT tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

An example of the IP tab in an SM with NAT enabled is displayed in Figure 90.

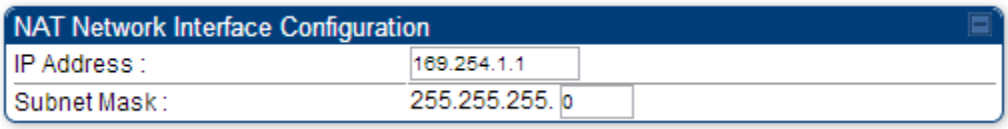


Figure 90: IP tab of SM with NAT enabled, example

In the IP tab of an SM with NAT enabled, you may set the following parameters.

NAT Network Interface Configuration, IP Address

Assign an IP address for SM management through Ethernet access to the SM. Set only the first three bytes. The last byte is permanently set to 1. This address becomes the base for the range of DHCP-assigned addresses.

NAT Network Interface Configuration, Subnet Mask

Assign a subnet mask of 255.255.255.0 or a more restrictive subnet mask. Set only the last byte of this subnet mask. Each of the first three bytes is permanently set to 255.

The IP tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

An example of the IP tab in an SM with NAT enabled is displayed in Figure 90.

Radio Tab of the SM

An example of the Radio tab in the SM is displayed in Figure 91.

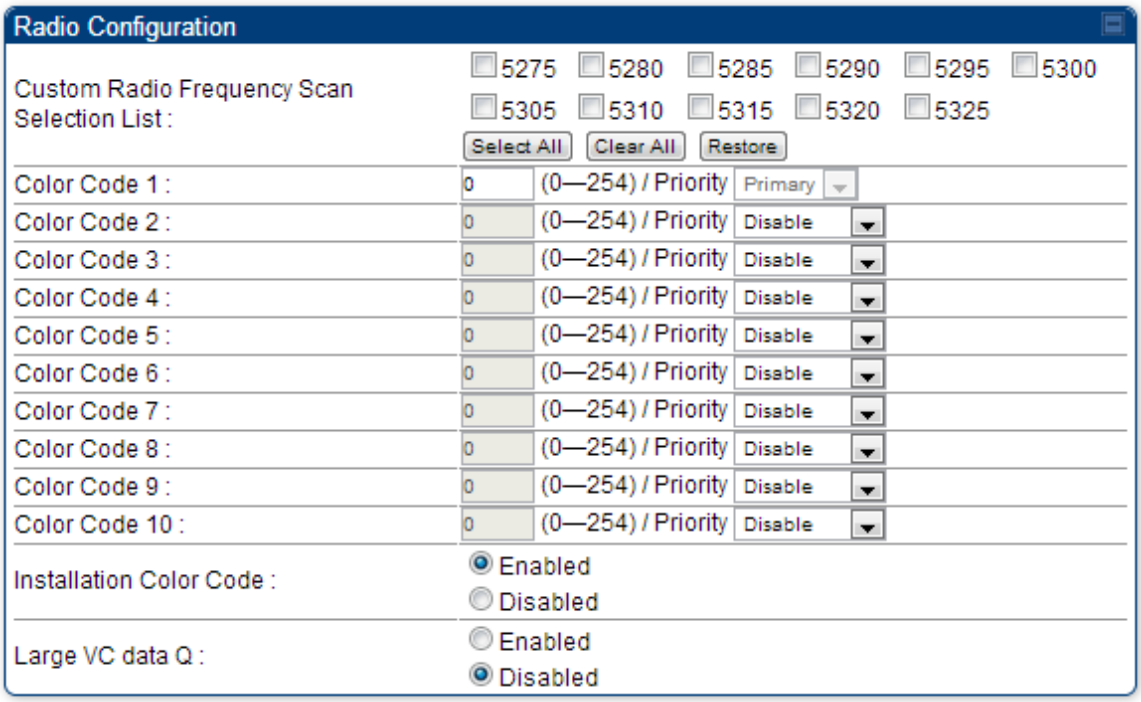

Radio Configuration
Custom Radio Frequency Scan Selection List :
5275 5280 5285 5290 5295 5300
5305 5310 5315 5320 5325
Select All
Clear All
Restore
Color Code 1 : 0 (0—254) / Priority Primary
Color Code 2 : 0 (0—254) / Priority Disable
Color Code 3 : 0 (0—254) / Priority Disable
Color Code 4 : 0 (0—254) / Priority Disable
Color Code 5 : 0 (0—254) / Priority Disable
Color Code 6 : 0 (0—254) / Priority Disable
Color Code 7 : 0 (0—254) / Priority Disable
Color Code 8 : 0 (0—254) / Priority Disable
Color Code 9 : 0 (0—254) / Priority Disable
Color Code 10 : 0 (0—254) / Priority Disable
Installation Color Code : Enabled Disabled
Large VC data Q : Enabled Disabled

Figure 91: Radio tab of SM, example

In the Radio tab of the SM, you may set the following parameters.

Custom Radio Frequency Scan Selection List

Check any frequency that you want the SM to scan for AP transmissions. The frequency *band* of the SM affects what channels you should select.

> ***IMPORTANT!***
> In the 2.4-GHz frequency band, the SM can register to an AP that transmits on a frequency 2.5 MHz higher than the frequency that the SM receiver locks when the scan terminates as successful. This establishes a poor-quality link. To prevent this, select frequencies that are at least 5 MHz apart.

In a 2.4-GHz SM, this parameter displays all available channels, but has only three recommended channels selected by default. See 2.4-GHz AP Cluster Recommended Channels on Page 136.

In a 5.2- or 5.4-GHz SM, this parameter displays only ISM frequencies. In a 5.7-GHz SM, this parameter displays both ISM and U-NII frequencies. If you select all frequencies that are listed in this field (default selections), then the SM scans for a signal on any channel. If you select only one, then the SM limits the scan to that channel. Since the frequencies that this parameter offers for each of these two bands are 5 MHz apart, a scan of *all* channels does not risk establishment of a poor-quality link as in the 2.4-GHz band.

A list of channels in the band is provided in Considering Frequency Band Alternatives on Page 134.

(The selection labeled **Factory** requires a special software key file for implementation.)

Color Code 1 to 10

Color code allows you to force the SM to register to only a specific AP, even where the SM can communicate with multiple APs. For registration to occur, the color code of the SM and the AP *must* match. Specify a value from 0 to 254.

Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).

RECOMMENDATION:
Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

SMs may be configured with up to 10 color codes. These color codes can be tagged as **Primary**, **Secondary**, or **Tertiary**, or **Disable**. When the SM is scanning for APs, it will first attempt to register to an AP that matches one of the SM's primary color codes. Failing that, the SM will continue scanning and attempt to register to an AP that matches one of the SM's secondary color codes. Failing that, the SM will continue scanning and attempt to register to an AP that matches one of the SM's tertiary color codes. This is all done in the scanning mode of the SM and will repeat until a registration has occurred.

Color codes in the same priority group are treated equally. For example, all APs matching one of the SM's primary color codes are analyzed equally. Likewise, this evaluation is done for the secondary and tertiary groups in order. The analysis for selecting an AP within a priority group is based on various inputs, including signal strength and number of SMs already registered to each AP.

The first color code in the configuration is the pre-Release 9.5 color code. Thus, it is always a primary color code for legacy reasons.

The color codes can be disabled, with the exception of the first color code.

Power Save Mode

P10 Board Types Only - This mode significantly economizes on power consumption, and **Enabled** is the default setting. Disable this feature only under guidance from technical support.

External Filters Delay

This parameter is present in only 900-MHz modules and can have effect in only those that have interference mitigation filter(s). If this value is present, leave it set to **0**, regardless of whether the SM has an interference mitigation filter.

Installation Color Code

With this feature enabled on the AP and SM, operators may install and remotely configure SMs without having to configure matching color codes between the modules. While the SM is accessible for configuration from above the AP (for remote provisioning) and below the SM (for local site provisioning), no user data is passed over the radio link. SMs with Installation Color Code enabled will first try any configured Color Code values first, then will use the Installation Color Code feature as a last result to connect to the AP. The status of the Installation Color Code can be viewed on the AP Eval web GUI page, and when the SM is registered using the Installation Color Code the message "SM is registered via ICC – Bridging Disabled!" is displayed in red on every SM GUI page. The Installation Color Code parameter is configurable without a radio reboot for both the AP and SM. If an SM is registered via Installation Color Code and the feature is then disabled, operators will need to reboot the SM or force it to reregister (i.e. using the **Rescan APs** functionality on the AP Eval page).

Large VC data Q

Certain applications such as video Surveillance cameras operate by sending bursts of IP traffic upstream. Some systems will send short bursts of packets at over 50 Mbps and then be idle for some period of time and then send another burst of data.

In order for the RF interface of a radio to accommodate these bursts of traffic, there is a configurable parameter on SM radios as well as BH Master and Slave radios to operate with a large input queue at the radio's data VC. This large queue allows packets which arrive at a rate greater than the radio link capacity to be stored in this deep queue until the radio is ready to transmit them. The queue size has been optimized to allow large packets to be stored just long enough so that there is always data available to be transmitted, but not large enough to cause packets to sit in a queue for a second or more.

Configuration of this parameter is shown on the Configuration => Radio web page on the SM, BHM and BHS. Operators should enable Large VC data Q on the BHM for downlink traffic or enable it on the BHS for uplink traffic.

If an operator is experiencing packet loss in the uplink due to bursting IP traffic and the overalltraffic rate is less than or equal to the uplink capacity of the radio system, then the large VC data Q should be enabled.

Transmitter Output Power

Nations and regions may regulate transmitter output power. For example

- Both 900-MHz and 5.7-GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance.

- Legal maximum allowable transmitter output power and EIRP (Equivalent Isotropic Radiated Power) in the 2.4-GHz frequency band varies by country and region. The output power of Series P9 2.4-GHz modules can be adjusted to meet these national or regional regulatory requirements.
- Countries and regions that permit the use of the 5.4-GHz frequency band (CEPT member states, for example), generally require equipment using the band to have adjustable power.

The professional installer of the equipment has the responsibility to

- maintain awareness of applicable regulations.
- calculate the permissible transmitter output power for the module.
- confirm that the initial power setting is compliant with national or regional regulations.
- confirm that the power setting is compliant following any reset of the module to factory defaults.

For information on how to calculate the permissible transmitter output power to enter in this parameter, see Adjusting Transmitter Output Power on Page 382.

In 5.4-GHz OFDM links, the operator sets the **Transmitter Output Power parameter** in the AP, and the AP then manages the transmitter output power of the SM appropriately.

The Radio tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

SNMP Tab of the SM

An example of the SNMP tab in an SM is displayed in Figure 92.

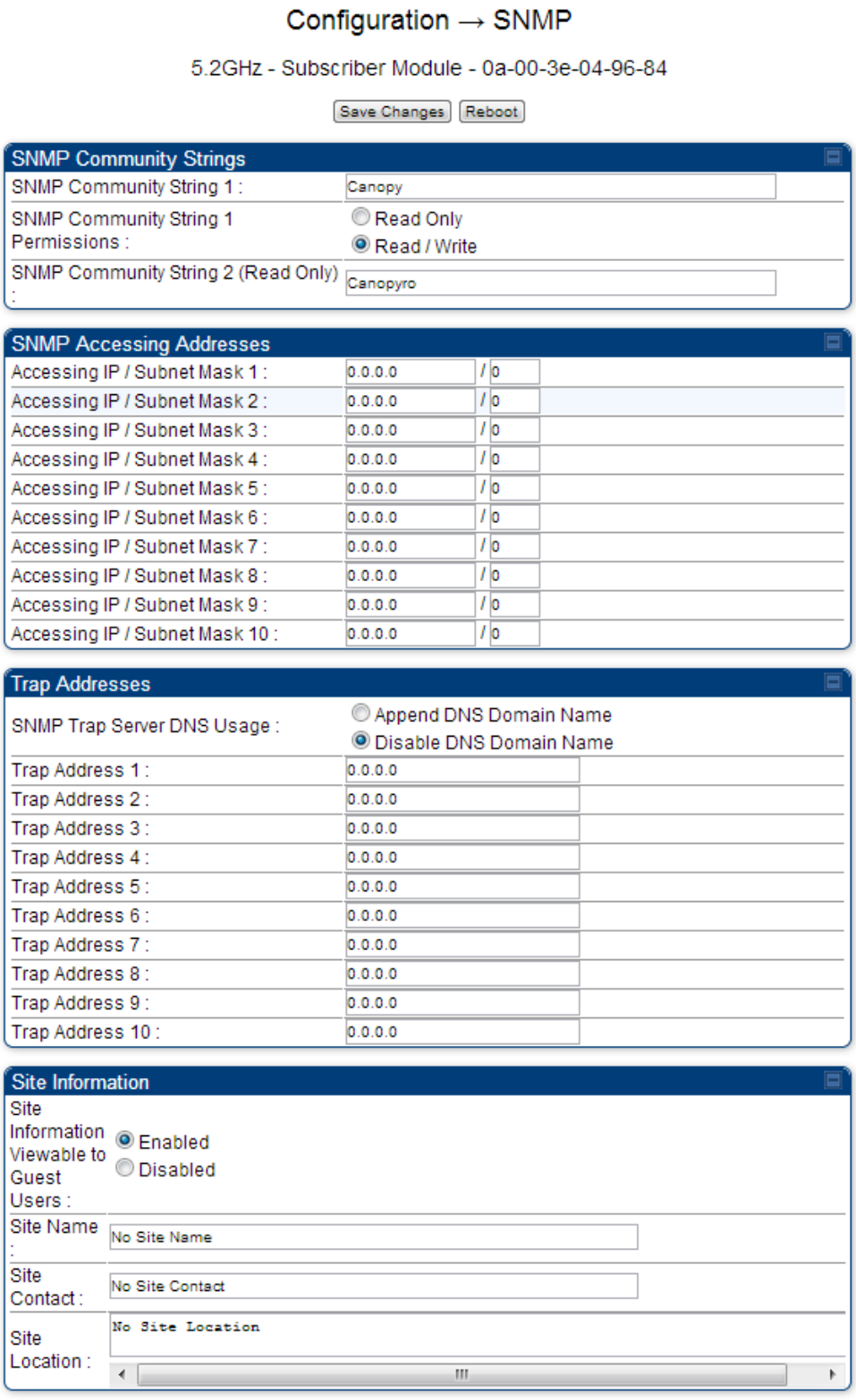

Configuration → SNMP
5.2GHz - Subscriber Module - 0a-00-3e-04-96-84
Save Changes
Reboot
SNMP Community Strings
SNMP Community String 1 :
Canopy
SNMP Community String 1 Permissions :
Read Only
Read / Write
SNMP Community String 2 (Read Only) :
Canopyro
SNMP Accessing Addresses
Accessing IP / Subnet Mask 1 :
Accessing IP / Subnet Mask 2 :
Accessing IP / Subnet Mask 3 :
Accessing IP / Subnet Mask 4 :
Accessing IP / Subnet Mask 5 :
Accessing IP / Subnet Mask 6 :
Accessing IP / Subnet Mask 7 :
Accessing IP / Subnet Mask 8 :
Accessing IP / Subnet Mask 9 :
Accessing IP / Subnet Mask 10 :
0.0.0.0 / 0
Trap Addresses
SNMP Trap Server DNS Usage :
Append DNS Domain Name
Disable DNS Domain Name
Trap Address 1 :
Trap Address 2 :
Trap Address 3 :
Trap Address 4 :
Trap Address 5 :
Trap Address 6 :
Trap Address 7 :
Trap Address 8 :
Trap Address 9 :
Trap Address 10 :
0.0.0.0
Site Information
Site Information Viewable to Guest Users :
Enabled
Disabled
Site Name :
No Site Name
Site Contact :
No Site Contact
Site Location :
No Site Location

Figure 92: SNMP tab of SM, example

In the SNMP tab of the SM, you may set the following parameters.

SNMP Community String 1

Specify a control string that can allow an Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is **Canopy**.

SNMP Community String 1 Permissions

You can designate the **SNMP Community String 1** to be the password for Prizm, for example, to have read/write access to the module via SNMP, or for all SNMP access to the module to be read only.

SNMP Community String 2 (Read Only)

Specify an additional control string that can allow an Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. The default string is **Canopy2**. This password will never authenticate a user or an NMS to read/write access.

The **Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **Accessing Subnet**, **Trap Address**, and **Permission** parameters.

Accessing IP / Subnet Mask *1 to 10*

Specify the addresses that are allowed to send SNMP requests to this SM. Prizm or the NMS has an address that is among these addresses (this subnet). You must enter both

- The network IP address in the form xxx.xxx.xxx.xxx
- The CIDR (Classless Interdomain Routing) prefix length in the form /xx

For example

- the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).
- 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the SM, presuming that the device supplies the correct **Community String** value.

The default treatment is to allow all networks access (set to 0). For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.” You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations.

RECOMMENDATION:
The subscriber can access the SM by changing the subscriber device to the accessing subnet. This hazard exists because the **Community String** and **Accessing Subnet** are both visible parameters. To avoid this hazard, configure the SM to filter (block) SNMP requests. See Filtering Protocols and Ports on Page 435.

SNMP Trap Server DNS Usage

The management DNS domain name may be toggled such that the name of the trap server only needs to be specified and the DNS domain name is automatically appended to that name. The default SNMP trap server addresses for all 10 available servers is 0.0.0.0 with the appending of the DNS domain name disabled.

Trap Address *1 to 10*

Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) to which trap information should be sent. Trap information informs Prizm or an NMS that something has occurred. For example, trap information is sent

- after a reboot of the module.
- when Prizm or an NMS attempts to access agent information but either
  - supplied an inappropriate community string or SNMP version number.
  - is associated with a subnet to which access is disallowed.

Site Information Viewable to Guest Users

Operators can enable or disable site information from appearing when a user is in GUEST account mode.

Site Name

Specify a string to associate with the physical module. This parameter is written into the *sysName* SNMP MIB-II object and can be polled by Prizm or an NMS. The buffer size for this field is 128 characters.

Site Contact

Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by Prizm or an NMS. The buffer size for this field is 128 characters.

Site Location

Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by Prizm or an NMS. The buffer size for this field is 128 characters.

The SNMP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Quality of Service (QoS) Tab of the SM

An example of the Quality of Service (QoS) tab in the SM is displayed in Figure 93.

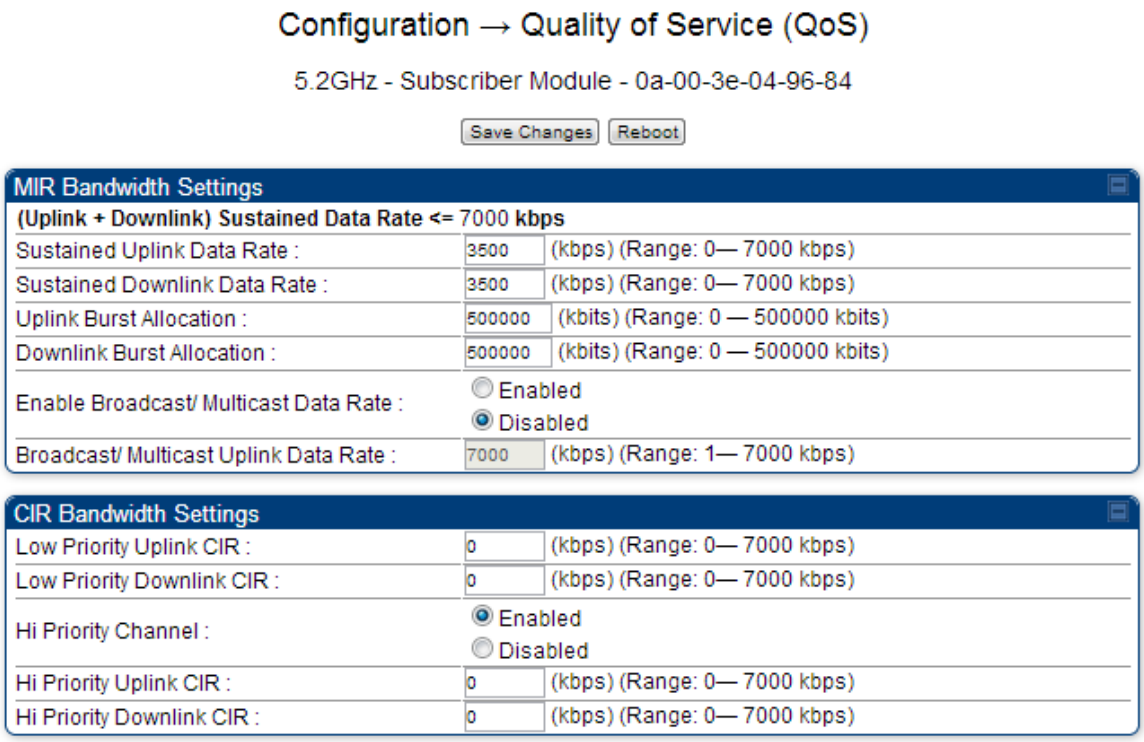

Configuration → Quality of Service (QoS)
5.2GHz - Subscriber Module - 0a-00-3e-04-96-84
Save Changes
Reboot
MIR Bandwidth Settings
(Uplink + Downlink) Sustained Data Rate <= 7000 kbps
Sustained Uplink Data Rate : 3500 (kbps) (Range: 0— 7000 kbps)
Sustained Downlink Data Rate : 3500 (kbps) (Range: 0— 7000 kbps)
Uplink Burst Allocation : 500000 (kbits) (Range: 0 — 500000 kbits)
Downlink Burst Allocation : 500000 (kbits) (Range: 0 — 500000 kbits)
Enable Broadcast/ Multicast Data Rate : Enabled Disabled
Broadcast/ Multicast Uplink Data Rate : 7000 (kbps) (Range: 1— 7000 kbps)
CIR Bandwidth Settings
Low Priority Uplink CIR : 0 (kbps) (Range: 0— 7000 kbps)
Low Priority Downlink CIR : 0 (kbps) (Range: 0— 7000 kbps)
Hi Priority Channel : Enabled Disabled
Hi Priority Uplink CIR : 0 (kbps) (Range: 0— 7000 kbps)
Hi Priority Downlink CIR : 0 (kbps) (Range: 0— 7000 kbps)

Figure 93: Quality of Service (QoS) tab of SM, example

In the Quality of Service (QoS) tab of the SM, you may set the following parameters.

Sustained Uplink Data Rate

Specify the rate that this SM is replenished with credits for transmission. This default imposes no restriction on the uplink. See

- Maximum Information Rate (MIR) Parameters on Page 83
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 86
- Setting the Configuration Source on Page 324.

Sustained Downlink Data Rate

Specify the rate at which the AP should be replenished with credits (tokens) for transmission to this SM. This default imposes no restriction on the uplink. See

- Maximum Information Rate (MIR) Parameters on Page 83
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 86
- Setting the Configuration Source on Page 324.

Uplink Burst Allocation

Specify the maximum amount of data to allow this SM to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more. See

- Maximum Information Rate (MIR) Parameters on Page 83
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 86
- Setting the Configuration Source on Page 324.

Downlink Burst Allocation

Specify the maximum amount of data to allow the AP to transmit to this SM before the AP is replenished at the **Sustained Downlink Data Rate** with transmission credits. See

- Maximum Information Rate (MIR) Parameters on Page 83
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 86
- Setting the Configuration Source on Page 324.

Low Priority Uplink CIR

See

- Committed Information Rate on Page 85
- Setting the Configuration Source on Page 324.

Low Priority Downlink CIR

See

- Committed Information Rate on Page 85
- Setting the Configuration Source on Page 324.

Hi Priority Channel

See

- High-priority Bandwidth on Page 86
- Setting the Configuration Source on Page 324.

Hi Priority Uplink CIR

See

- High-priority Bandwidth on Page 86
- Committed Information Rate on Page 85
- Setting the Configuration Source on Page 324.

Hi Priority Downlink CIR

See

- High-priority Bandwidth on Page 86
- Committed Information Rate on Page 85
- Setting the Configuration Source on Page 324.

The Quality of Service (QoS) tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made in this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Security Tab of the SM

An example of the Security tab in an SM is displayed in Figure 94.

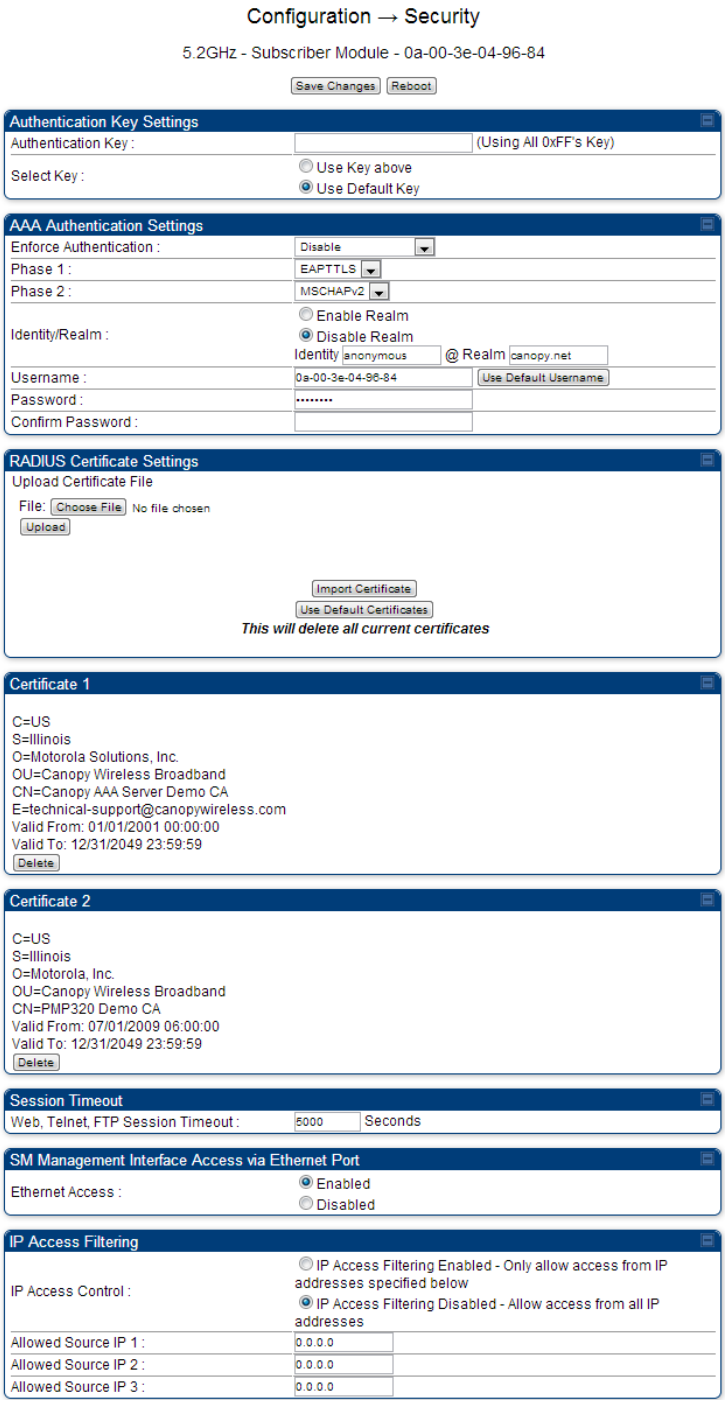


Figure 94: Security tab of SM, example

In the Security tab of the SM, you may set the following parameters.

Authentication Key

Only if the AP to which this SM will register requires authentication, specify the key that the SM should use when authenticating. For alpha characters in this hex key, use only upper case.

Select Key

The **Use Default Key** selection specifies the predetermined key for authentication in Wireless Manager

The **Use Key above** selection specifies the 32-digit hexadecimal key that is permanently stored on both the SM and the WM

Enforce Authentication

The SM may enforce authentication types of **AAA** and **AP Pre-sharedKey**. The SM will not finish the registration process if the AP is not using the configured authentication method (and the SM will lockout the AP for 15 minutes).

Phase 1

The protocols supported for the **Phase 1** (Outside Identity) phase of authentication are EAPTTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) or MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2).

Phase 2

Select the desired **Phase 2** (Inside Identity) authentication protocol from the **Phase 2** options of **PAP** (Password Authentication Protocol), **CHAP** (Challenge Handshake Authentication Protocol), and **MSCHAP (**Microsoft's version of CHAP, version 2 is used). The protocol must be consistent with the authentication protocol configured on the RADIUS server.

Identity/Realm

If Realms are being used, select **Enable Realm** and configure an outer identity in the **Identity** field and a Realm in the **Realm** field. These must match the Phase 1/Outer Identity and Realm configured in the RADIUS server. The default **Identity** is "anonymous". The **Identity** can be up to 128 non-special (no diacritical markings) alphanumeric characters. The default **Realm** is "canopy.net". The **Realm** can also be up to 128 non-special alphanumeric characters.

Configure an outer Identity in the **Username** field. This must match the Phase 1/Outer Identity username configured in the RADIUS server. The default Phase 1/Outer Identity **Username** is "anonymous". The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.

Username

Enter a **Username** for the SM. This must match the username configured for the SM on the RADIUS server. The default **Username** is the SM's MAC address. The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.

Password

Enter the desired password for the SM in the **Password** and **Confirm Password** fields**..** The **Password** must match the password configured for the SM on the RADIUS server. The default **Password** is "password". The **Password** can be up to 128 non-special (no diacritical markings) alphanumeric characters

Upload Certificate File

To upload a certificate manually to an SM, first load it in a known place on your PC or network drive, then click on a **Delete** button on one of the Certificate description blocks to delete a certificate to provide space for your certificate. Click on **Choose File,** browse to the location of the certificate, and click the **Import Certificate** button, and then reboot the radio to use the new certificate.

When a certificate is in use, after the SM successfully registers to an AP, an indication of **In Use** will appear in the description block of the certificate being used.

The public certificates installed on the SMs are used with the private certificate on the RADIUS server to provide a public/private key encryption system.

Up to 2 certificates can be resident on an SM. An installed certificate can be deleted by clicking the **Delete** button in the certificate's description block on the Configuration > Security tab. To restore fhe 2 default certificates, click the **Use Default Certificates** button in the **RADIUS Certificate Settings** parameter block and reboot the radio.

Web, Telnet, FTP Session Timeout

Enter the expiry in seconds for remote management sessions via HTTP, telnet, or FTP access to the SM.

Ethernet Access Control

If you want to prevent any device that is connected to the Ethernet port of the SM from accessing the management interface of the SM, select **Ethernet Access Disabled**. This selection disables access through this port to via http (the GUI), SNMP, telnet, ftp, and tftp. With this selection, management access is available through only the RF interface via either an IP address (if **Network Accessibility** is set to **Public** on the SM) or the Session Status or Remote Subscribers tab of the AP.

This setting does not prevent a device connected to the Ethernet port from accessing the management interface of *other SMs* in the network. To prevent this, use the **IP Access Filtering Enabled** selection in the **IP Access Control** parameter of the SMs in the network. See **IP Access Control** below.

If you want to allow management access through the Ethernet port, select **Ethernet Access Enabled**. This is the factory default setting for this parameter.

IP Access Control

You can permit access to the SM from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address

Allowed Source IP *1 to 3*

If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the SM from any IP address. You may populate as many as all three.

If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.

VLAN Tab of the SM

An example of the VLAN tab in an SM is displayed in Figure 95.

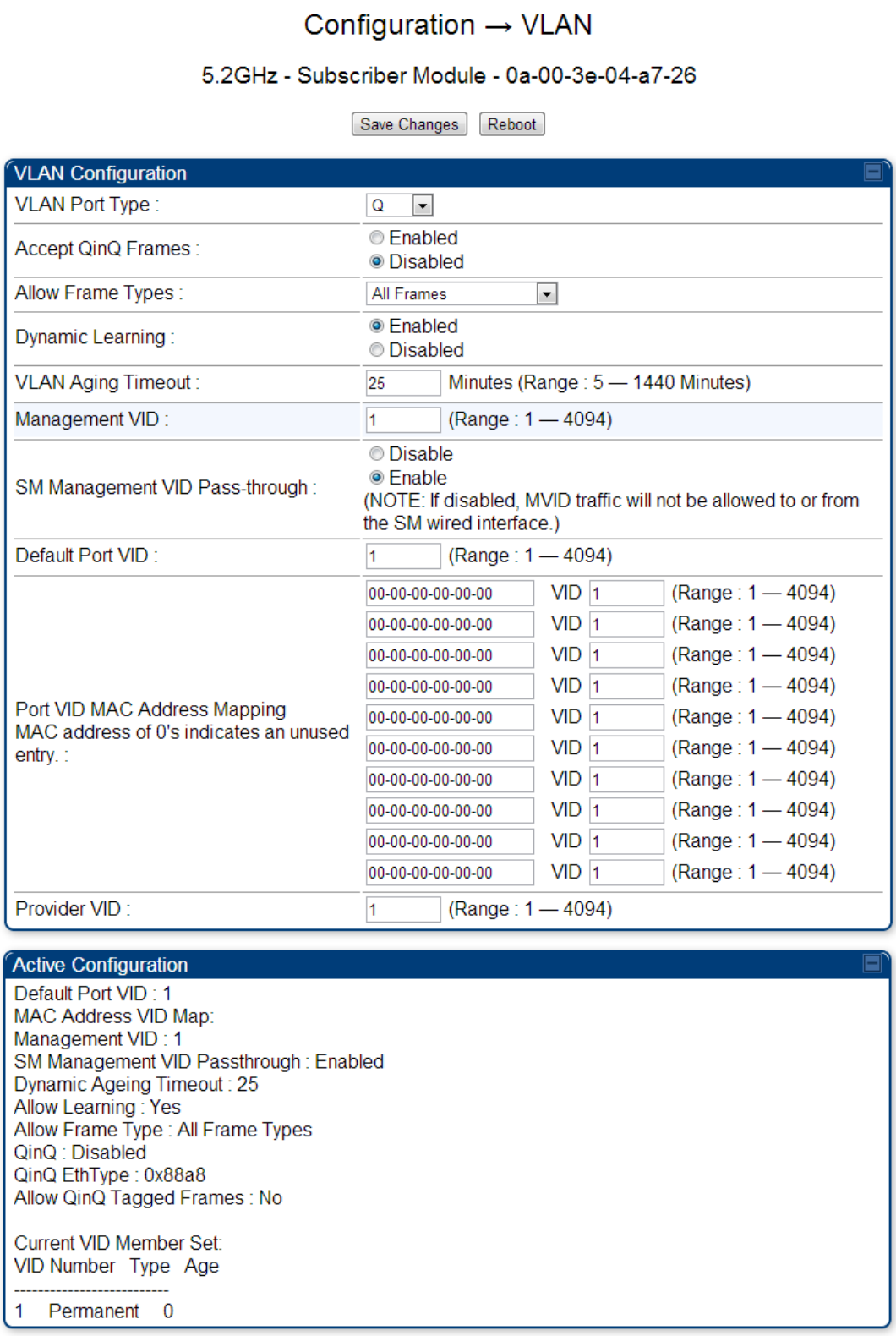


Figure 95: VLAN tab of SM, example

In the VLAN tab of an SM, you may set the following parameters.

Always use Local VLAN Config

Enable this option before you reboot this AP as an SM to use it to perform spectrum analysis. After the spectrum analysis is completed and before you reboot this module as an AP, disable this option.

VLAN Port Type

By default this will be simply Q, indicating that it is to operate in the existing manner. The other option is Q-in-Q, which indicates that it should be adding and removing the S-Tag, and adding a C-Tag if necessary for untagged packets. The VLAN Port type corresponds to the Ethernet port of the SM. Currently, the internal management interfaces will always operate as Q ports.

Accept QinQ Frames

This option is valid for the Q-in-Q port so that the user may force blocking of existing 802.1ad Q-in-Q frames. This way, only untagged or single tagged packets will come in and out of the Ethernet interface. If a Q-in-Q frame is about ingress or egress the Ethernet interface and this is disabled, it will be dropped and a filter entry will show up on the VLAN Statistics page as DVLAN Egress or DVLAN Ingress.

Dynamic Learning

Specify whether the SM should (**Enable**) or should not (**Disable**) add the VIDs of upstream frames (that enter the SM through the wired Ethernet interface) to the VID table. The default value is **Enable**.

Allow Frame Types

Select the type of arriving frames that the SM should tag, using the VID that is stored in the **Untagged Ingress VID** parameter. The default value is **All Frames**.

VLAN Aging Timeout

Specify how long the SM should keep dynamically learned VIDs. The range of values is 5 to 1440 (minutes). The default value is **25** (minutes).

NOTE:
VIDs that you enter for the **Untagged Ingress VID** and **Management VID** parameters do not time out.

Management VID

Enter the VID that the SM should share with the AP. The range of values is 1 to 4095. The default value is **1**.

SM Management VID Pass-through

Specify whether to allow the SM (**Enable**) or the AP (**Disable**) to control the VLAN settings of this SM. The default value is **Enable**.

When VLAN is enabled in the AP to whom this SM is registered, the Active Configuration block provides the following details as read-only information in this tab. In the Cambium fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

Default Port VID

This is the VID that will be used for untagged frames and will correspond to the Q-Tag for 802.1Q frames (if VLAN Port Type is Q), or the C-Tag for 802.1ad frames (if the VLAN Port Type is Q-in- Q).

Port VID MAC Address Mapping

These parameters allow operators to place specific devices onto different VLANs (802.1Q tag or 802.1ad C-tag) based on the source MAC address of the packet. If the MAC address entry is 00-00-00-00-00-00 then that entry is not used. If a packet arrives at the SM that is sourced from a device whose MAC address is in the table, then the corresponding VID will be used for that frame's Q-tag (Q port) or C-tag (Q-in-Q port). If there is no match, then the Default Port VID will be used. This table is also used in the downstream direction for removal of the tag based on the destination MAC address so that an untagged (for Q port) or Q-Tagged (for Q-in-Q port) frame is delivered to the end device. You may use wildcards for the non-OUI (Organizationally Unique Identifier) portion of the MAC address, which is the last 3 bytes. MAC addresses contain 6 bytes, the first 3 of which are the OUI of the vendor that manufactured the device and the last 3 are unique to that vendor OUI. If you want to cover all devices from a known vendor's OUI, you would specify 0xFF for the remaining 3 bytes. So, for example, if you wanted all devices from a specific vendor with an OUI of 00-95-5b (which is a Netgear OUI) to be on the same VID of 800, you would specify an entry with MAC address 00-95-5b-ff-ff-ff. Then, any device underneath of the SM with MAC addresses starting with 00-95-5b will be put on VLAN 800.

Provider VID

The provider VID is used for the S-tag. It is only used if the **Port Type** is **Q-in-Q** and will always be used for the S-tag. If an existing 802.1Q frame arrives, the **Provider VID** is what will be used for adding and removing of the outer S-tag. If an untagged frame arrives to a Q-in-Q port, then the **Provider VID** will be the S-tag and the **Default Port VID** (or **Port VID MAC Address Mapping**, if valid) will be used for the C-tag.

Default Port VID

This is the value of the parameter of the same name, configured above.

MAC Address VID Map

This is the listing of the MAC address VIDs configured in **Port VID MAC Address Mapping**.

Management VID

This is the value of the parameter of the same name, configured above.

SM Management VID Pass-Through

This is the value of the parameter of the same name, configured above.

Dynamic Ageing Timeout

This is the value of the **VLAN Aging Timeout** parameter configured above.

Allow Learning

Yes is displayed if the value of the **Dynamic Learning** parameter above is **Enabled**. No is displayed if the value of **Dynamic Learning** is **Disabled**.

Allow Frame Type

This displays the selection that was made from the drop-down list at the **Allow Frame Types** parameter above.

QinQ

This is set to Enabled if VLAN Port Type is set to QinQ, and is set to Disabled if VLAN Port Type is set to Q.

QinQ EthType

This is the value of the QinQ EtherType configured in the AP.

Allow QinQ Tagged Frames

This is the value of **Accept QinQ Frames**, configured above.

Current VID Member Set, VID Number

This column lists the ID numbers of the VLANs in which this module is a member, whether through assignment or through dynamic learning.

Current VID Member Set, Type

For each VID number in the first column, the entry in this column correlates the way in which the module became and continues to be a member:

- **Permanent**—This indicates that the module was assigned the VID number through direct configuration by the operator.
- **Dynamic**—This indicates that the module adopted the VID number through enabled dynamic learning, when a tagged packet from an SM behind it in the network, or from a customer equipment that is behind the SM in this case, was read.

Current VID Member Set, Age

For each VID number in the first column of the table, the entry in this column reflects whether or when the VID number will time out:

- for **Permanent** type—the number will never time out, and this is indicated by the digit 0.
- for **Dynamic** type—the **Age** reflects what is configured in the **VLAN Aging Timeout** parameter in the Configuration => VLAN tab of the AP or reflects a fewer number of minutes that represents the difference between what was configured and what has elapsed since the VID was learned. Each minute, the Age decreases by one until, at zero, the AP deletes the learned VID, but can it again from packets sent by elements that are beneath it in the network.

IMPORTANT!

Values in this Active Configuration block can differ from attempted values in configurations:

- A VLAN profile administered by the BAM subsystem in Prizm is capable of overriding any configured VLAN value, if the **Configuration Source** parameter in the AP is set to BAM.
- The AP can override the value that the SM has configured for **SM Management VID Pass-Through**.

The VLAN tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

VLAN Membership Tab of the SM

An example of the VLAN Membership tab in an SM is displayed in Figure 96.

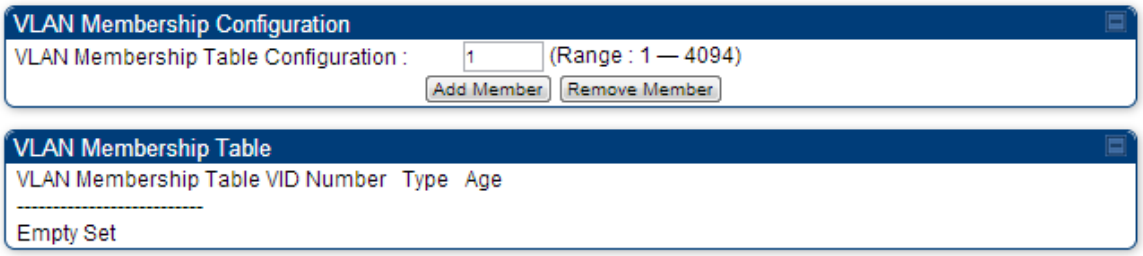


Figure 96: VLAN Membership tab of SM, example

In the VLAN Membership tab, you may set the following parameter.

VLAN Membership Table Configuration

For each VLAN in which you want the AP to be a member, enter the VLAN ID and then click the **Add Member** button. Similarly, for any VLAN in which you want the AP to no longer be a member, enter the VLAN ID and then click the **Remove Member** button.

Diffserv Tab of the SM

An example of the Diffserv tab in an SM is displayed in Figure 97.

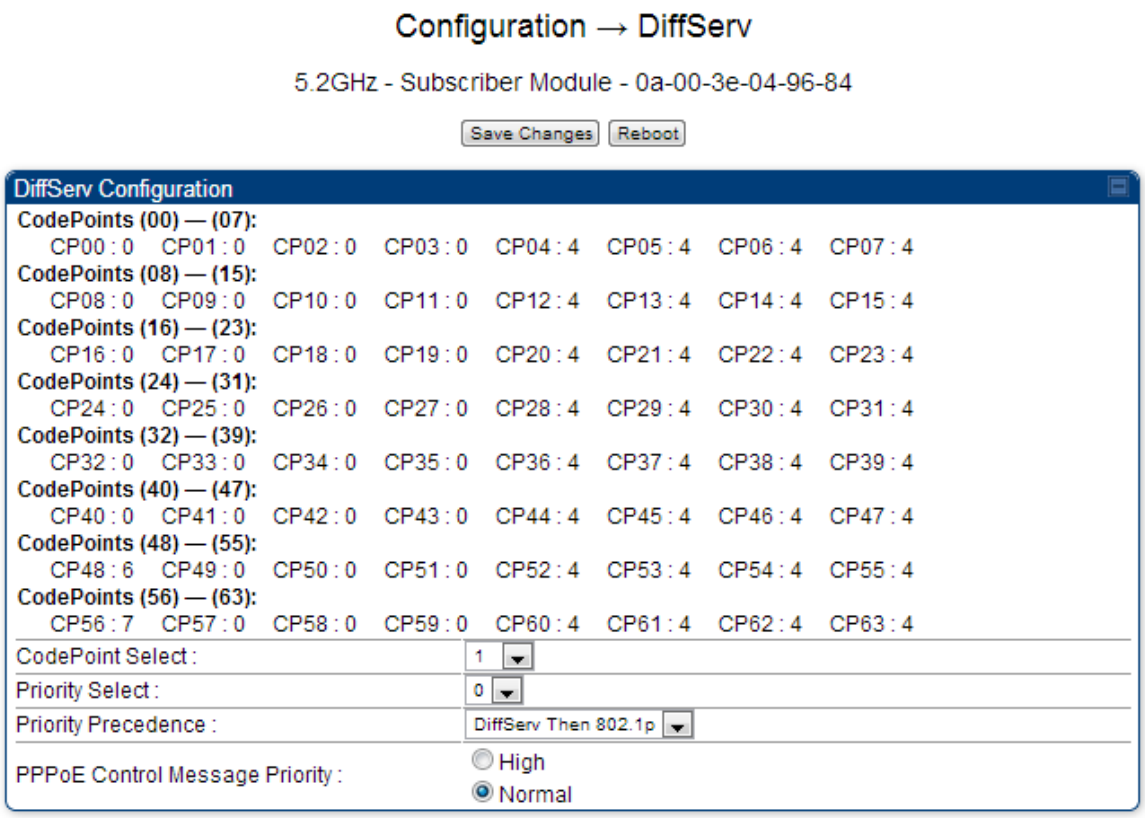

Configuration → DiffServ
5.2GHz - Subscriber Module - 0a-00-3e-04-96-84
Save Changes
Reboot
DiffServ Configuration
CodePoints (00) — (07):
CP00 : 0 CP01 : 0 CP02 : 0 CP03 : 0 CP04 : 4 CP05 : 4 CP06 : 4 CP07 : 4
CodePoints (08) — (15):
CP08 : 0 CP09 : 0 CP10 : 0 CP11 : 0 CP12 : 4 CP13 : 4 CP14 : 4 CP15 : 4
CodePoints (16) — (23):
CP16 : 0 CP17 : 0 CP18 : 0 CP19 : 0 CP20 : 4 CP21 : 4 CP22 : 4 CP23 : 4
CodePoints (24) — (31):
CP24 : 0 CP25 : 0 CP26 : 0 CP27 : 0 CP28 : 4 CP29 : 4 CP30 : 4 CP31 : 4
CodePoints (32) — (39):
CP32 : 0 CP33 : 0 CP34 : 0 CP35 : 0 CP36 : 4 CP37 : 4 CP38 : 4 CP39 : 4
CodePoints (40) — (47):
CP40 : 0 CP41 : 0 CP42 : 0 CP43 : 0 CP44 : 4 CP45 : 4 CP46 : 4 CP47 : 4
CodePoints (48) — (55):
CP48 : 6 CP49 : 0 CP50 : 0 CP51 : 0 CP52 : 4 CP53 : 4 CP54 : 4 CP55 : 4
CodePoints (56) — (63):
CP56 : 7 CP57 : 0 CP58 : 0 CP59 : 0 CP60 : 4 CP61 : 4 CP62 : 4 CP63 : 4
CodePoint Select :
1
Priority Select :
0
Priority Precedence :
DiffServ Then 802.1p
PPPoE Control Message Priority :
High
Normal

Figure 97: Diffserv tab of SM, example

In the Diffserv tab of the SM, you may set the following parameters.

CodePoint 1 through CodePoint 47

The default priority value for each settable CodePoint is shown in Figure 118. Priorities of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities.

Consistent with RFC 2474

- **CodePoint 0** is predefined to a fixed priority value of **0** (low-priority channel).
- **CodePoint 48** is predefined to a fixed priority value of **6** (high-priority channel).
- **CodePoint 56** is predefined to a fixed priority value of **7** (high-priority channel).

You cannot change any of these three fixed priority values. Among the settable parameters, the priority values (and therefore the handling of packets in the high- or low-priority channel) are set in the AP for all downlinks within the sector and in the SM for each uplink. See DSCP Field on Page 87.

CodePoint 49 through CodePoint 55

CodePoint 57 through CodePoint 63

The Diffserv tab of the SM also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Protocol Filtering Tab of the SM

An example of the Protocol Filtering tab in an SM is displayed in Figure 98.

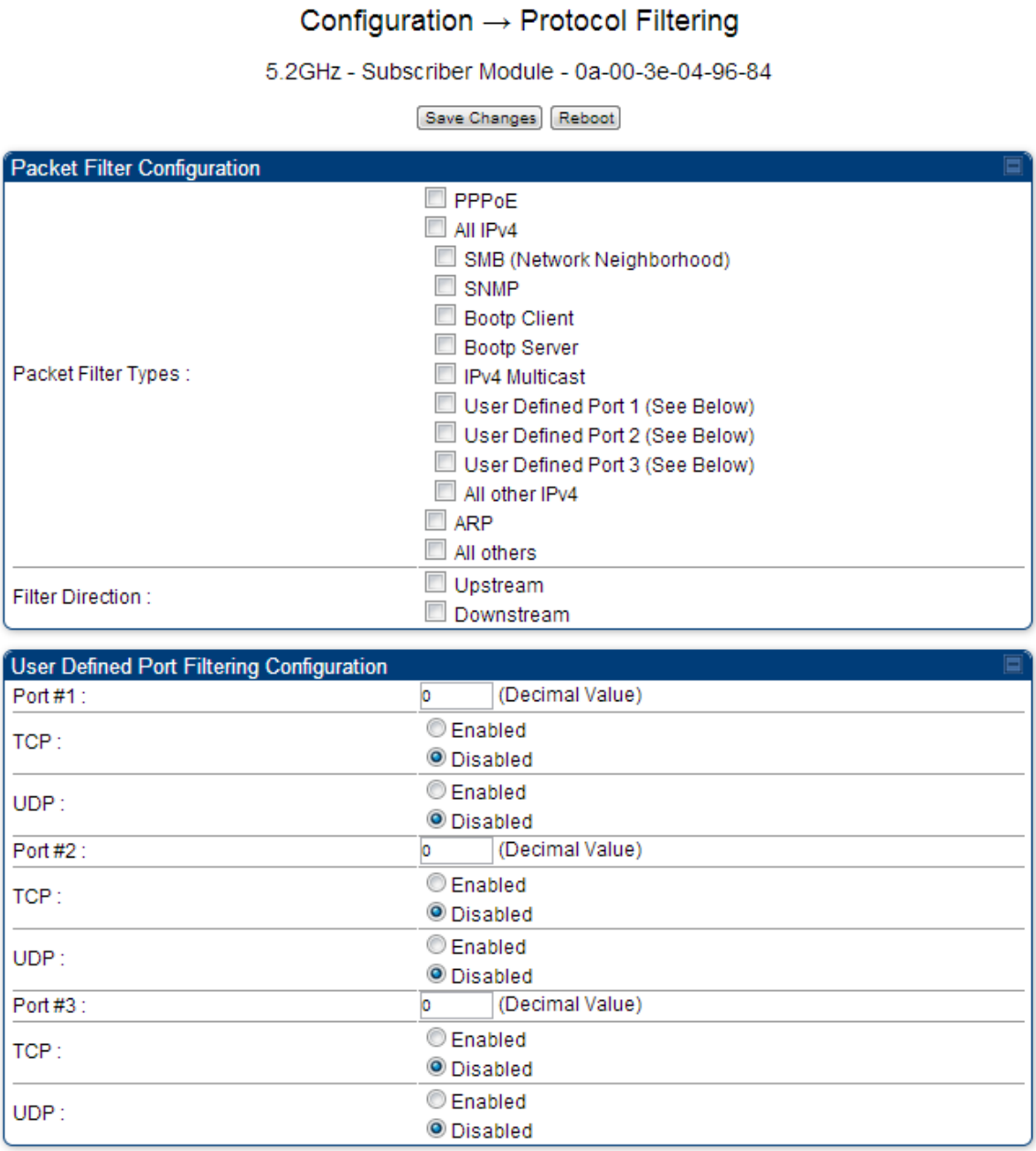


Figure 98: Protocol Filtering tab of SM, example

In the Protocol Filtering tab of the SM, you may set the following parameters.

Packet Filter Types

For any box selected, the Protocol and Port Filtering feature blocks the associated protocol type. Examples are provided in Protocol and Port Filtering with NAT Disabled on Page 436.

To filter packets in any of the user-defined ports, you must do all of the following:

- Check the box for User Defined Port *n* (See Below) in the Packet Filter Types section of this tab.
- In the User Defined Port Filtering Configuration section of this tab, both
  - provide a port number at **Port #*n***.
  - check **TCP**, **UDP**, or both.

If the **DHCP state** parameter is set to **Enabled** in the Configuration => IP tab of the SM, *do not* check the **Bootp Client** option for **Packet Filter Types** in its Protocol Filtering tab, because doing so would block the DHCP request. (Filters apply to all packets that leave the SM via its RF interface, including those that the SM itself generates.) If you want to keep DHCP enabled and avoid the blocking scenario, select the **Bootp Server** option instead. This will result in responses being appropriately filtered and discarded.

Filter Direction

Select which direction of traffic should be filtered – Upstream (uplink) or Downstream (downlink).

User Defined Port Filtering Configuration

You can specify ports for which to block subscriber access, regardless of whether NAT is enabled. For more information, see Filtering Protocols and Ports on Page 435.

PPPoE Tab of the SM

An example of the PPPoE tab of the SM is displayed in Figure 99.

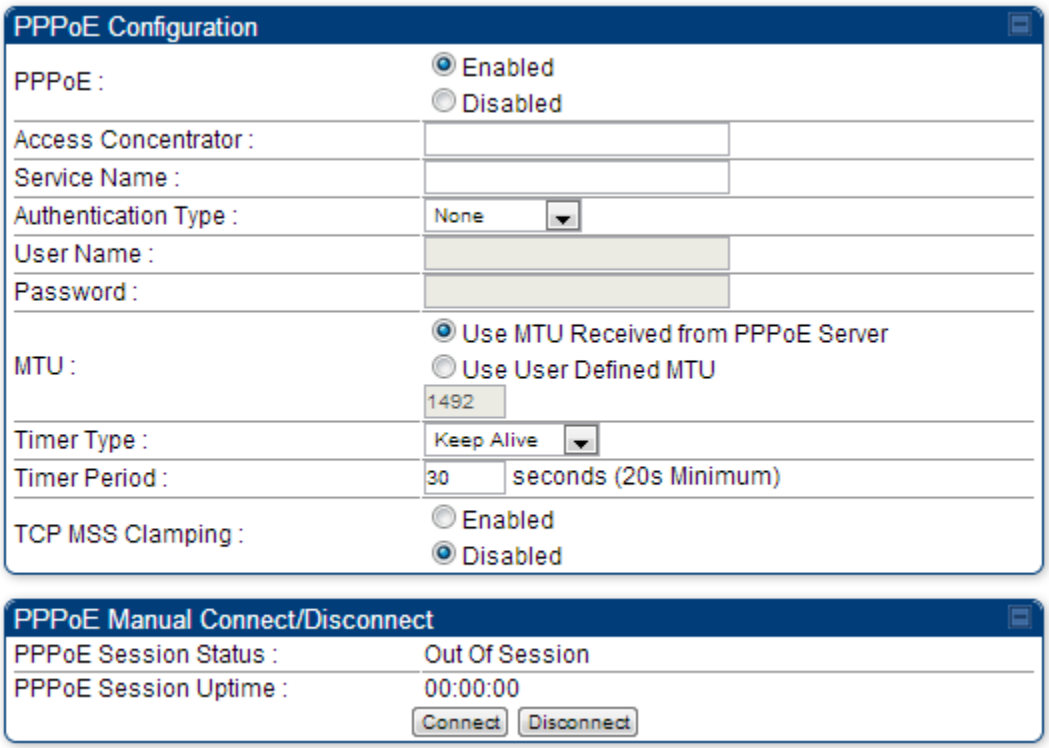


Figure 99: PPPoE tab of SM, example

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a protocol that encapsulates PPP frames inside Ethernet frames (at Ethernet speeds). Benefits to the network operator may include

- Access control
- Service monitoring
- Generation of statistics about activities of the customer
- Re-use of infrastructure and operational practices by operators who already use PPP for other networks

PPPoE options are configurable for the SM only, and the AP indicates whether or not PPPoE is enabled for a specific subscriber.

When PPPoE is enabled, once the RF session comes up between the SM and the AP, the SM will immediately attempt to connect to the PPPoE Server. You can monitor the status of this by viewing the PPPoE Session Log in the Logs section (Administrator only). Every time the RF session comes up, the SM will check the status of the link and if it is down, the SM will attempt to redial the link if necessary depending on the Timer Type. Also, on the Configuration page, the user may Connect or Disconnect the session manually. This can be used to override the session to force a manual disconnect and/or reconnect if there is a problem with the session.

In order to enable PPPoE, NAT MUST be enabled on the SM, and Translation Bridging MUST be disabled on the AP. These items will be strictly enforced for you when you are trying to enable PPPoE. A message will indicate any prerequisites not being met. Also, the NAT Public IP DHCP client cannot be enabled This is because the NAT Public IP will be received through the IPCP process of the PPPoE discovery stages.

The pre-requisites required are:

- NAT MUST be enabled on the SM
  - NAT DHCP Client will be disabled automatically. The NAT public IP will be received from the PPPoE Server.
  - NAT Public Network Interface Configuration will not be used and should be left to defaults. Also NAT Public IP DHCP will be disabled if it is enabled.
- Translation Bridging MUST be DISABLED on the AP
  - This will only be determined if the SM is in session since the SM won't know the AP configuration otherwise. If the SM is not in session, PPPoE can be enabled but if the SM goes into session to a Translation Bridge-enabled AP, then PPPoE will not be enabled.

The following PPPoE configuration options are available:

Access Concentrator

An optional entry to set a specific access concentrator to connect to for the PPPoE session. If this is blank, the SM will accept the first access concentrator which matches the service name (if specified). This is limited to 32 characters.

Service Name

An optional entry to set a specific service name to connect to for the PPPoE session. If this is left blank the SM will accept the first service option that comes back from the access concentrator specified above, if any. This is limited to 32 characters.

Authentication Type

- **None** means that no PPPoE authentication will be implemented
- **CHAP/PAP** means that CHAP authentication will be attempted first, then PAP authentication. The same password is used for both types.

User Name

This is the CHAP/PAP user name that will be used if CHAP/PAP authentication is selected. If **None** is selected for authentication then this field is unused. This is limited to 32 characters.

Password

This is the CHAP/PAP password that will be used if PAP authentication is selected. If **None** is selected for authentication then this field is unused. This is limited to 32 characters.

MTU

- **Use MTU Received from PPPoE Server** causes the SM to use the MRU of the PPPoE server received in LCP as the MTU for the PPPoE link.
- **Use User Defined MTU** allows the operator to specify an MTU value to use to override any MTU that may be determined in the LCP phase of PPPoE session setup. If this is selected, the user will be able to enter an MTU value up to 1492. However, if the MTU determined in LCP negotiations is less than this user-specified value, the SM will use the smaller value as its MTU for the PPPoE link.

Timer Type

- **Keep Alive** is the default timer type. This timer will enable a keepalive that will check the status of the link periodically. The user can set a keepalive period. If no data is seen from the PPPoE server for that period, the link will be taken down and a reconnection attempt will be started. For marginal links, the keep alive timer can be useful so that the session will stay alive over periodic dropouts. The keepalive timer should be set such that the session can outlast any session drop. Some PPPoE servers will have a session check timer of their own so that the timeouts of the server and the SM should be in sync so that one side does not drop the session prematurely.
- **Idle Timeout** enables an idle timer that will check the usage of the link from the customer side. If there is no data seen from the customer for the idle timeout period, the PPPoE session will be dropped. Once data starts flowing from the customer again, the session will be started up again. This timer is useful for users who may not be using the connection frequently. If the session is idle for long periods of time, this timer will allow the resources used by the session to be returned to the server. Once the connection is used again by the customer, the link will be reestablished automatically.

Timer Period

The length in seconds of the PPPoE keepalive timer.

TCP MSS Clamping

If this is enabled, then the SM will alter TCP SYN and SYN-ACK packets by changing the Maximum Segment Size to be compatible with the current MTU of the PPPoE link. This way, the user does not have to worry about MTU on the client side for TCP packets. The MSS will be set to the current MTU – 40 (20 bytes for IP headers and 20 bytes for TCP headers). This will cause the application on the client side to not send any TCP packets larger than the MTU. If the network is exhibiting large packet loss, try enabling this option. This may not be an option on the PPPoE server itself. The SM will NOT reassemble IP fragments, so if the MTUs are incorrect on the end stations, then MSS clamping will solve the problem for TCP connections.

PPPoE Session Status

This field indicates the current PPPoE session status, for easy reference.

PPPoE Session Uptime

This field indicates the total uptime of the current PPPoE session.

NAT Port Mapping Tab of the SM

An example of the NAT Port Mapping tab in an SM is displayed in Figure 100.

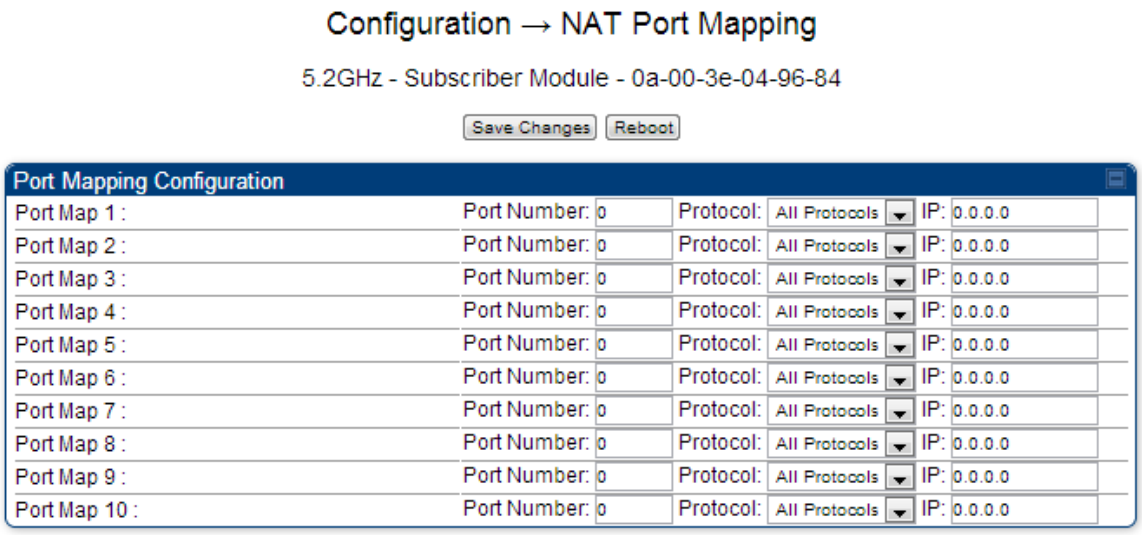

Configuration → NAT Port Mapping
5.2GHz - Subscriber Module - 0a-00-3e-04-96-84
Save Changes
Reboot
Port Mapping Configuration
Port Map 1 : Port Number: 0 Protocol: All Protocols IP: 0.0.0.0
Port Map 2 : Port Number: 0 Protocol: All Protocols IP: 0.0.0.0
Port Map 3 : Port Number: 0 Protocol: All Protocols IP: 0.0.0.0
Port Map 4 : Port Number: 0 Protocol: All Protocols IP: 0.0.0.0
Port Map 5 : Port Number: 0 Protocol: All Protocols IP: 0.0.0.0
Port Map 6 : Port Number: 0 Protocol: All Protocols IP: 0.0.0.0
Port Map 7 : Port Number: 0 Protocol: All Protocols IP: 0.0.0.0
Port Map 8 : Port Number: 0 Protocol: All Protocols IP: 0.0.0.0
Port Map 9 : Port Number: 0 Protocol: All Protocols IP: 0.0.0.0
Port Map 10 : Port Number: 0 Protocol: All Protocols IP: 0.0.0.0

Figure 100: NAT Port Mapping tab of SM, example

In the NAT Port Mapping tab of the SM, you may set the following parameters.

Port Map *1 to 10*

Separate parameters allow you to distinguish NAT ports from each other by assigning a unique combination of port number, protocol for traffic through the port, and IP address for access to the port.

Unit Settings Tab of the SM

An example of the Unit Settings tab in an SM is displayed in Figure 101.

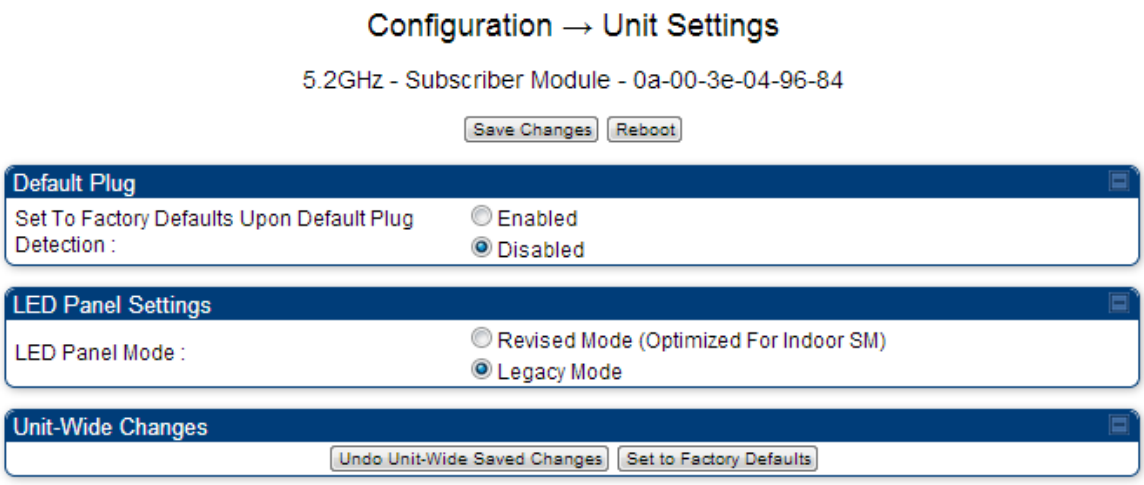


Figure 101: Unit Settings tab of SM, example

The Unit Settings tab of the SM contains an option for how the SM should react when it detects a connected override plug. You may set this option as follows.

Set to Factory Defaults Upon Default Plug Detection

If **Enabled** is checked, then an override/default plug functions as a default plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all parameter values are reset to defaults. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *cannot* see or learn the settings that were previously configured in it. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the default values for any that were not.

If **Disabled** is checked, then an override/default plug functions as an override plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all previously configured parameter values remain and are displayed. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *can* see and learn the settings. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the previous values for any that were not.

See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 433.

LED Panel Mode

Optionally select Revised Mode for simpler use of the LEDs during alignment of the SM. See Diagnostic LEDs on Page 185.

The Unit Settings tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Unit-Wide Saved Changes

When you click this button, any changes that you made in any tab but did not commit by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all tabs* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Setting the Configuration Source

The AP includes a **Configuration Source** parameter, which sets where SMs that register to the AP are controlled for MIR, VLAN, the high-priority channel, and CIR as follows.
The **Configuration Source** parameter affects the source of

- all MIR settings:
  - Sustained Uplink Data Rate
  - Uplink Burst Allocation
  - Sustained Downlink Data Rate
  - Downlink Burst Allocation
- all SM VLAN settings:
  - Dynamic Learning
  - Allow Only Tagged Frames
  - VLAN Ageing Timeout
  - Untagged Ingress VID
  - Management VID
  - VLAN Membership
- the Hi Priority Channel setting
- all CIR settings
  - Low Priority Uplink CIR
  - Low Priority Downlink CIR
  - Hi Priority Uplink CIR
  - Hi Priority Downlink CIR

Most operators whose plans are typical should consult Table 53.

Table 53: Recommended combined settings for typical operations

Most operators who use…	should set this parameter…	in this web page / tab…	in the AP to…
no authentication server	**Authentication Mode**	Configuration/ Security	**Disabled**
	Configuration Source	Configuration/ General	**SM**
Wireless Manager (Authentication Server)	**Authentication Mode**	Configuration/ Security	**Authentication Server**
	Configuration Source	Configuration/ General	**Authentication Server**
RADIUS AAA server	**Authentication Mode**	Configuration/ Security	**RADIUS AAA**
	Configuration Source	Configuration/ General	**Authentication Server**

Operators whose plans are atypical should consider the results that are described in Table 54 and Table 55. For any SM whose **Authentication Mode** parameter is set to **Authentication Required**, the listed settings are derived as shown in Table 54.

Table 54: Where feature values are obtained for an SM with authentication required

Configuration Source Setting in the AP	Values are obtained from			
	MIR Values	**VLAN Values**	**High Priority Channel State**	**CIR Values**
Authentication Server	Authentication Server	Authentication Server	Authentication Server	Authentication Server
SM	SM	SM	SM	SM
Authentication Server+SM	Authentication Server	Authentication Server, then SM	Authentication Server, then SM	Authentication Server, then SM

NOTES:

HPC represents the **Hi Priority Channel** (enable or disable).

Where *BAM, then SM* is the indication, parameters for which BAM does not send values are obtained from the SM. This is the case where the BAM server is operating on a BAM release that did not support the feature. This is also the case where the feature enable/disable flag in BAM is set to disabled. The values are those previously set or, if none ever were, then the default values.

Where *BAM* is the indication, values in the SM are disregarded.

Where *SM* is the indication, values that BAM sends for the SM are disregarded.

The high-priority channel is unavailable to Series P7 and P8 SMs.

For any SM whose **Authentication Mode** parameter *is not* set to **Authentication Required**, the listed settings are derived as shown in Table 55.

Table 55: Where feature values are obtained for an SM with authentication disabled

Configuration Source Setting in the AP	Values are obtained from			
	MIR Values	**VLAN Values**	**High Priority Channel State**	**CIR Values**
Authentication Server	AP	AP	AP	AP
SM	SM	SM	SM	SM
Authentication Server+SM	SM	SM	SM	SM

BAM Release 2.0 sends only MIR values. BAM Release 2.1 and Prizm Release 2.0 and 2.1 send VLAN and high-priority channel values as well.

For the case where the **Configuration Source** parameter in the AP is set to **Authentication Server**, the SM stores a value for the **Dynamic Learning** VLAN parameter that differs from its factory default. When Prizm does not send VLAN values (because **VLAN Enable** is set to **No** in Prizm), the SM

- uses this stored **Disable** value for **Dynamic Learning**.
- shows the following in the VLAN Configuration web page:
  - *either* **Enable** *or* **Disable** as the value of the **Dynamic Learning** parameter.

- **Allow Learning : No** under **Active Configuration**.

For the case where the **Configuration Source** parameter in the AP is set to **Authentication Server+SM**, and Prizm does not send VLAN values, the SM

- uses the configured value in the SM for **Dynamic Learning**. If the SM is set to factory defaults, then this value is **Enable**.
- shows under **Active Configuration** the result of the configured value in the SM. For example, if the SM is set to factory defaults, then the VLAN Configuration page shows **Allow Learning : Yes**.

This selection (**Authentication Server+SM**) *is not* recommended where Prizm manages the VLAN feature in SMs.

Configuring a BH Timing Master for the Destination

NOTE:
The PTP 400 and PTP 600 series bridges (previously known as 30/60 Mbps and 150/300 Mbps Backhauls) are described in their own dedicated user guides. See Products Not Covered by This User Guide on Page 24.

If an ADMINISTRATOR-level password has been set in the BHM, you must log into the module before you can configure its parameters. See Managing Module Access by Passwords on Page 430.

General Tab of the BHM

An example of the General tab in a BHM is displayed in Figure 102.

Figure 102: General tab of BHM, example

In the General tab of the BHM, you may set the following parameters.

Timing Mode

Select **Timing Master**. This BH will provide sync for the link. Whenever you toggle this parameter to Timing Master from Timing Slave, you should also do the following:

1. Make no other changes in this or any other interface page.
2. Save this change of timing mode.

3. Reboot the BH.

RESULT: The set of interface web pages that is unique to a BHM is made available.

Link Speed

From the drop-down list of options, select the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all APs, BHs, and SMs in the operator network.

Sync Input

Specify the type of synchronization for this BH timing master to use.

- Select **Sync to Received Signal (Power Port)** to set this BHM to receive sync from a connected CMMmicro or CMM4.
- Select **Sync to Received Signal (Timing Port)** to set this BHM to receive sync from a connected CMM2, an AP in the cluster, an SM, or a BH timing slave.
- Select **Generate Sync Signal** where the BHM does not receive sync, and no AP or other BHM is active within the link range.

Verify GPS Message Checksum

When enabled (Sync Input “Sync to Received Signal (Timing Port)” must be selected for this parameter to display), the device validates GPS messaging to ensure that the radio is properly receiving data from the GPS source. If a GPS source is not calculating and sending checksum data properly, the BHM will still receive synchronization pulses but not GPS data (location, data, etc.) and the Invalid Message counter will increase on the radio’s Home > GPS Status page. If an BHM is receiving synchronization properly from a GPS unit but is not receiving GPS data, operators may set **Verify GPS Message Checksum** to “Disabled” to ignore checksum failures and to allow the BHM to process the GPS data.

Region Code

From the drop-down list, select the region in which the radio is operating.
When the appropriate region is selected in this parameter, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard. For further information on DFS, see Radar Signature Detection and Shutdown on Page 127.

Unlike selections in other parameters, your **Region Code** selection requires a **Save Changes** and a **Reboot** cycle before it will force the context-sensitive GUI to display related options (for example, **Alternate Frequency Carrier *1 and 2*** in the Configuration => Radio tab). Thus, a proper configuration exercise in environments that are subject to DFS requirements has two imperative **Save Changes** and **Reboot** cycles: one after the **Region Code** is set, and a second after related options are set.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

Bridge Entry Timeout

Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.

CAUTION!
An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.

Bridging Functionality

Select whether you want bridge table filtering active (**Enable**) or not (**Disable**) on this BHM. Selecting **Disable** allows you to use redundant BHs without causing network addressing problems. Through a spanning tree protocol, this reduces the convergence time from 25 minutes to mere seconds. However, you should disable bridge table filtering as only a deliberate part of your overall network design. Otherwise, disabling it allows unwanted traffic across the wireless interface.

Update Application Address

For capabilities in future software releases, you can enter the address of the server to access for software updates on this BHM.

Dynamic Rate Adapt

See 2X Operation on Page 89.

Prioritize TCP ACK

To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements. This parameter, when enabled, can be particularly useful when running bi-direction FTP sessions over the link. If a link is primarily used for video surveillance, it is recommended to configure this parameter to “Disabled”. See AP-SM Links on Page 99.

Multicast Destination Address

Using Link Layer Discovery Protocol (LLDP), a module exchanges multicast addresses with the device to which it is wired on the Ethernet interface. Although some switches (CMMmicro, for example) do not pass LLDP addresses upward in the network, a radio can pass it as the value of the **Multicast Destination Address** parameter value in the connected device that has it populated.

In this way, an SM can report to Prizm, for example, the multicast address of a connected remote AP, and thus allow Prizm to discover that AP. To allow this, set the message mode in the remote AP to **LLDP Multicast**. Set this parameter in the BHM to **Broadcast**. The SM will pass this address in broadcast mode, and the CMMmicro will pass the address upward in the network, since it does not discard addresses that it receives in broadcast mode.

Where the AP is not behind another device, the **Broadcast** mode will allow discovery of the AP.

Coordinates

Physical radio location data may be configured via the Latitude, Longitude, and Height fields.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

IP Tab of the BHM

An example of an IP tab in a BHM is displayed in Figure 103.

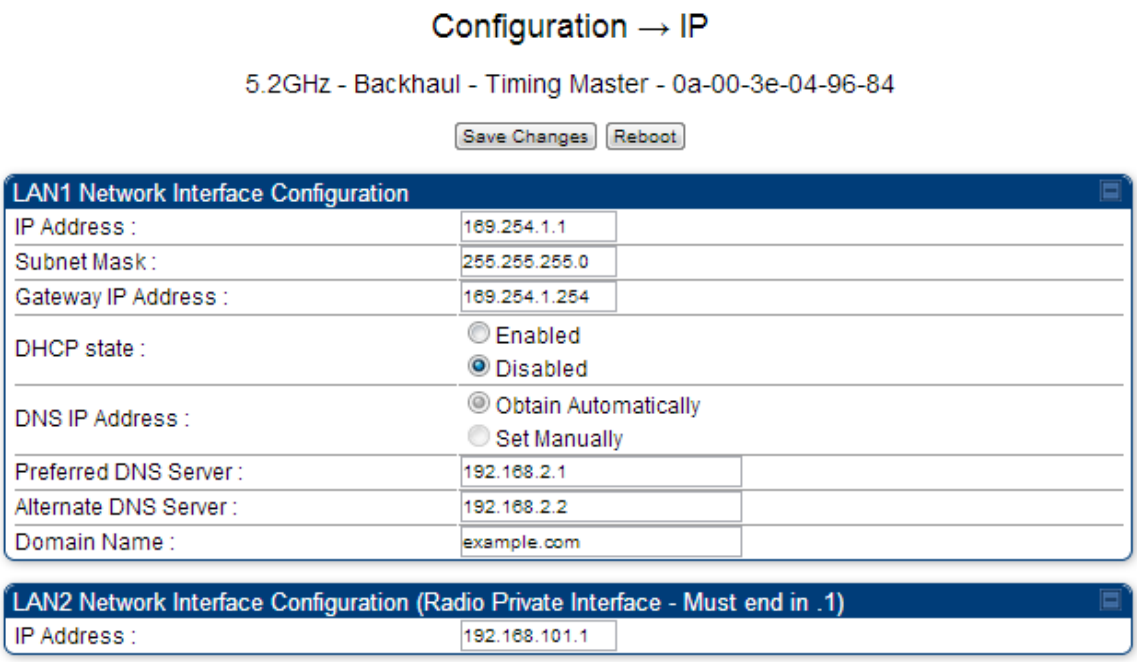


Figure 103: IP tab of BHM, example

You may set the following IP Configuration page parameters.

LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to be associated with the Ethernet connection on this module. (The default IP address from the factory is 169.254.1.1.) If you set and then forget this parameter, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 433.

RECOMMENDATION:
Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the BHM to communicate on the network. The default subnet mask is 255.255.0.0. See Allocating Subnets on Page 164.

LAN1 Network Interface Configuration, Gateway IP Address

Enter the appropriate gateway for the BHM to communicate with the network. The default gateway is 169.254.0.0.

LAN1 Network Interface Configuration, DHCP State

If you select **Enabled**, the DHCP server automatically assigns the IP configuration (IP address, subnet mask, and gateway IP address) and the values of those individual parameters (above) are not used. The setting of this DHCP state parameter is also viewable, but not settable, in the Network Interface tab of the Home page.

LAN1 Network Interface Configuration, DNS IP Address

Canopy devices allow for configuration of a preferred and alternate DNS server IP address either automatically or manually. Devices must set DNS server IP address manually when DHCP is disabled for the management interface of the device. DNS servers may be configured automatically from the DHCP response when DHCP is enabled for the management interface of the device. Optionally devices may be configured to set the DNS server IP address manually when DHCP is enabled for the management interface. The default DNS IP addresses are 0.0.0.0 when configured manually.

LAN1 Network Interface Configuration, Preferred DNS Server

The first address used for DNS resolution.

LAN1 Network Interface Configuration, Alternate DNS Server

Upon failure to reach the Preferred DNS server, the Alternate DNS Server is used.

LAN1 Network Interface Configuration, Domain Name

The operator's management domain name may be configured for DNS. The domain name configuration can be used for configuration of the servers in the operator's network. The default domain name is example.com, and is only used if configured as such.

LAN2 Network Interface Configuration (RF Private Interface), IP Address

Enter the IP address to be associated with this BHM for over-the-air access.

The IP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the IP Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Radio Tab of the BHM

An example of the Radio tab in a BHM is displayed in Figure 104.

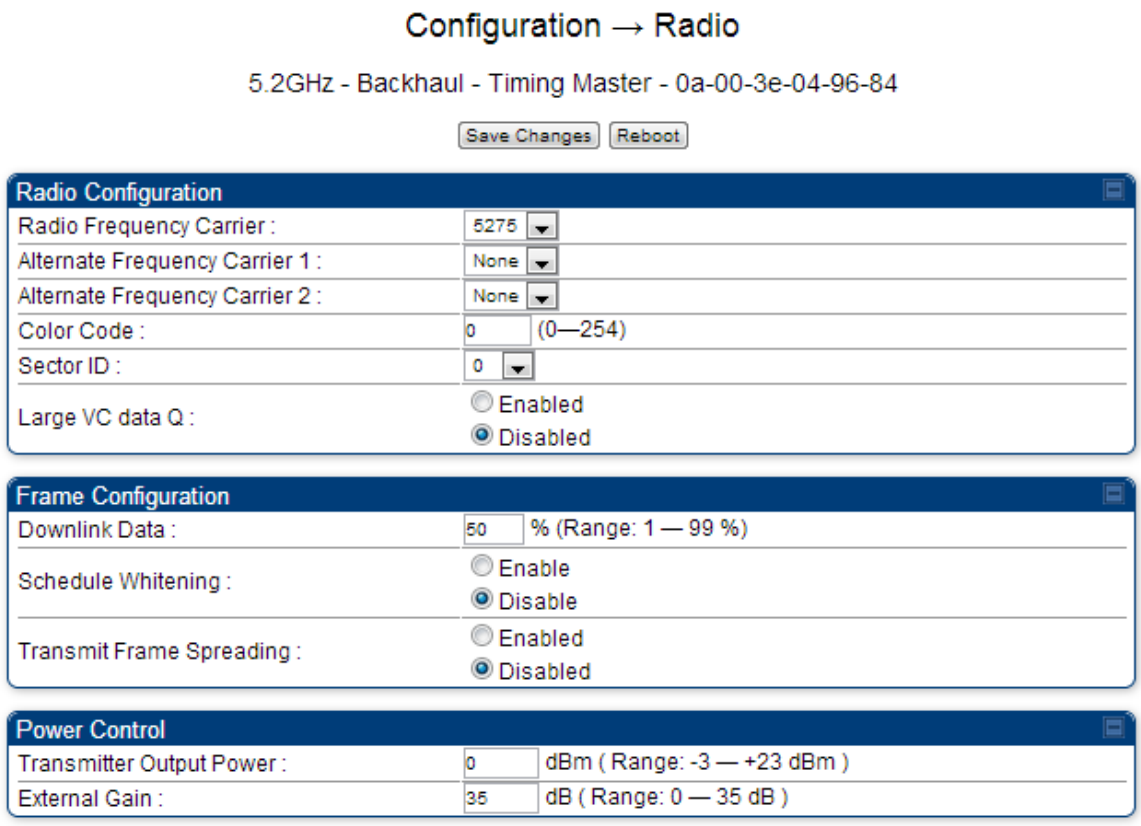


Figure 104: Radio tab of BHM, example

In the Radio tab of the BHM, you may set the following parameters.

Radio Frequency Carrier

Specify the frequency for the BHM to transmit. The default for this parameter is **None**. (The selection labeled **Factory** requires a special software key file for implementation.)
In a 5.7-GHz BHM, this parameter displays both ISM and U-NII frequencies. In a 5.2-GHz BHM, this parameter displays only ISM frequencies. For a list of channels in the band, see Considering Frequency Band Alternatives on Page 134.

Alternate Frequency Carrier 1

If your network operates in a region in which DFS shutdown capability is required, and you do not see this parameter, perform the following steps:

1. Click the General tab.
2. Set the **Region Code** parameter from its drop-down list.
3. Click the **Save Changes** button.
4. Click the **Reboot** button.
5. Click the Radio tab.

From the drop-down list, select the frequency that the BHM should switch to if it detects a radar signature on the frequency configured in the **Radio Frequency Carrier** parameter. See Radar Signature Detection and Shutdown on Page 127.

Alternate Frequency Carrier 2

From the drop-down list, select the frequency that the BHM should switch to if it detects a radar signature on the frequency configured in the **Alternate Frequency Carrier 1** parameter. See Radar Signature Detection and Shutdown on Page 127.

Color Code

Specify a value from 0 to 254. For registration to occur, the color code of the BHM and the BHS *must* match. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).

RECOMMENDATION:
Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

Sector ID

You can optionally enter an identifier to distinguish this link.

Large VC data Q

Certain applications such as video Surveillance cameras operate by sending bursts of IP traffic upstream. Some systems will send short bursts of packets at over 50 Mbps and then be idle for some period of time and then send another burst of data.

In order for the RF interface of a radio to accommodate these bursts of traffic, there is a configurable parameter on SM radios as well as BH Master and Slave radios to operate with a large input queue at the radio's data VC. This large queue allows packets which arrive at a rate greater than the radio link capacity to be stored in this deep queue until the radio is ready to transmit them. The queue size has been optimized to allow large packets to be stored just long enough so that there is always data available to be transmitted, but not large enough to cause packets to sit in a queue for a second or more.

Configuration of this parameter is shown on the Configuration => Radio web page on the SM, BHM and BHS. Operators should enable Large VC data Q on the BHM for downlink traffic or enable it on the BHS for uplink traffic.

If an operator is experiencing packet loss in the uplink due to bursting IP traffic and the overalltraffic rate is less than or equal to the uplink capacity of the radio system, then the large VC data Q should be enabled.

For example, a PTP 20 Mbps BH has a video camera connected to the BH Slave (BHS) uplink. To check if packets are being lost at the BHS RF interface the operator should check the "outdiscards Count" at the Statistics->Radio page of the BHS. If this count is incrementing, then packets are being lost at the RF interface of the BHS and the Large VC data Q should be enabled. In the figure below, the outdiscards Count shows 455 discard events since the counter was reset, indicating that probably system performance would be improved by the Large VC data Q.

Power Save Mode

P10 Board Types Only - Select either

- **Enabled** (the default), to reduce module power consumption by approximately 10% without affecting the transmitter output power. This is the recommended setting.
- **Disabled**, to continue normal power consumption, but only under guidance from technical support.

Downlink Data

The operator specifies the percentage of the aggregate (uplink and downlink total) throughput that is needed for the downlink. The default for this parameter is 50%.

Schedule Whitening

Select either

- **Enable**, to spread the transmitted signal power to avoid peaks that modules with Dynamic Frequency Selection (DFS) configured might interpret as radar. This is the recommended setting.
- **Disable**, to allow peaks in transmitted signal power.

PTP 200 Series (OFDM) BHMs do not support this parameter.

Transmit Frame Spreading

If you select **Enable**, then a BHS between two BHMs can register in the assigned BHM (not the other BHM). Cambium *strongly recommends* that you select this option. With this selection, the BHM does not transmit a beacon in each frame, but rather transmits a beacon in only pseudo-random frames in which the BHS expects the beacon. This allows multiple BHMs to send beacons to multiple BHSs in the same range without interference.

Transmitter Output Power

Nations and regions may regulate transmitter output power. For example

- 5.7-GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance.
- Legal maximum allowable transmitter output power and EIRP (Equivalent Isotropic Radiated Power) in the 2.4-GHz frequency band varies by country and region. The output power of Series P9 2.4-GHz modules can be adjusted to meet these national or regional regulatory requirements.
- Countries and regions that permit the use of the 5.4-GHz frequency band (CEPT member states, for example), generally require equipment using the band to have adjustable power. In the PTP54200 OFDM BHM, transmitter output power is settable in the range of −30 to 15 dBm. However, with only the integrated antenna, where regulation[8] requires that EIRP is not greater than 27 dBm, compliance requires that the transmitter output power is set to 10 dBm or less. With a 12 dBi external antenna on the connectorized version of this BHM, the full range (up to 15 dBm) is acceptable.

The professional installer of the equipment has the responsibility to

- maintain awareness of applicable regulations.
- calculate the permissible transmitter output power for the module.
- confirm that the initial power setting is compliant with national or regional regulations.

[8] This is the case in most regions, including the U.S.A., Europe, and Canada.

- confirm that the power setting is compliant following any reset of the module to factory defaults.

For information on how to calculate the permissible transmitter output power to enter in this parameter, see Adjusting Transmitter Output Power on Page 382.

External Gain

If your network operates in a region in which DFS shutdown capability is required, and you do not see this parameter, perform the following steps:

1. Click the General tab.
2. Set the **Region Code** parameter from its drop-down list.
3. Click the **Save Changes** button.
4. Click the **Reboot** button.
5. Click the Radio tab.

Using Table 56 as a guide, type in the dB value by which to reduce Dynamic Frequency Selection (DFS) sensitivity to radar signals.

Table 56: Recommended External Gain values for AP

Module Type	Recommended Setting
FSK with only integrated patch antenna	0
FSK with 9 dB Canopy LENS	9
FSK with standard 18 dB reflector	18
FSK connectorized with 15.5 dBi antenna and 0.5 dB cable loss	15
OFDM with only integrated antenna	17
OFDM connectorized with antenna that was purchased with it	17
OFDM connectorized with separately purchased antenna	antenna gain minus coax + connector loss

The value of this parameter does not affect transmitter output power. This parameter is present in only radios that support DFS and hence is not present in 900-MHz radios.

The Radio tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the IP Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

SNMP Tab of the BHM

An example of the SNMP tab in a BHM is displayed in Figure 105.

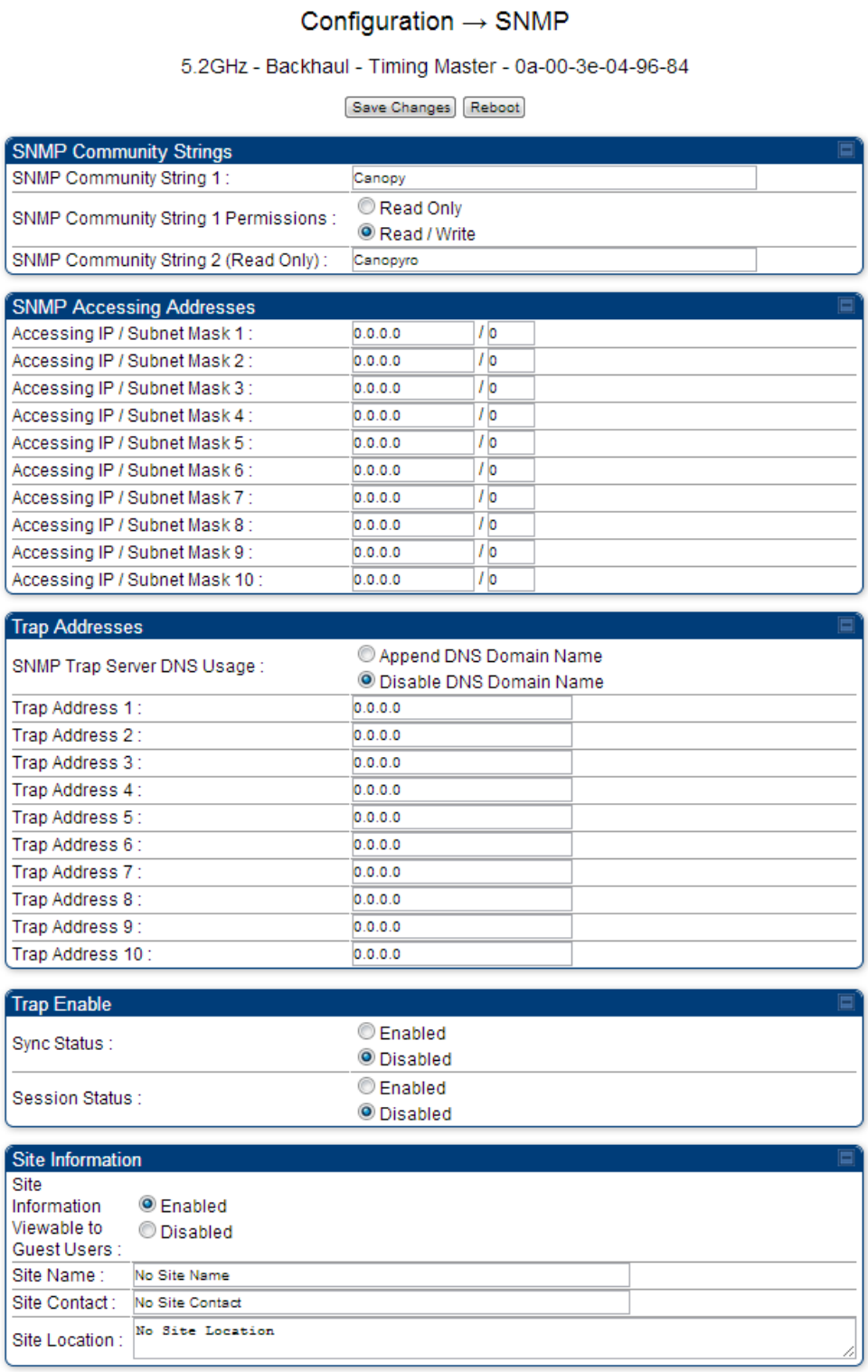


Figure 105: SNMP tab of BHM, example

In the SNMP tab of the BHM, you may set the following parameters.

SNMP Community String 1

Specify a control string that can allow an Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is **Canopy**.

SNMP Community String 1 Permissions

You can designate the **SNMP Community String 1** to be the password for Prizm, for example, to have read/write access to the module via SNMP, or for all SNMP access to the module to be read only.

SNMP Community String 2 (Read Only)

Specify an additional control string that can allow an Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. The default string is **Canopy2**. This password will never authenticate a user or an NMS to read/write access.

The **Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **Accessing Subnet**, **Trap Address**, and **Permission** parameters.

Accessing IP / Subnet Mask *1 to 10*

Specify the addresses that are allowed to send SNMP requests to this BHM. Prizm or the NMS has an address that is among these addresses (this subnet). You must enter both

- The network IP address in the form xxx.xxx.xxx.xxx
- The CIDR (Classless Interdomain Routing) prefix length in the form /xx

For example

- the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).
- 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the BHM, presuming that the device supplies the correct **Community String** value.

NOTE:
For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.”

The default treatment is to allow all networks access. You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations.

SNMP Trap Server DNS Usage

The management DNS domain name may be toggled such that the name of the trap server only needs to be specified and the DNS domain name is automatically appended to that name. The default SNMP trap server addresses for all 10 available servers is 0.0.0.0 with the appending of the DNS domain name disabled.

Trap Address *1 to 10*

Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) to which trap information should be sent. Trap information informs Prizm or an NMS that something has occurred. For example, trap information is sent

- after a reboot of the module.
- when Prizm or an NMS attempts to access agent information but either
  - supplied an inappropriate community string or SNMP version number.
  - is associated with a subnet to which access is disallowed.

Sync Status

If you want sync status traps (sync lost and sync regained) sent to Prizm or an NMS, select **Enabled**. If you want these traps suppressed, select **Disabled**.

Session Status

If you want session status traps sent to Prizm or an NMS, select **Enabled**. For the names and descriptions of session status traps, see Traps Provided in the Canopy Enterprise MIB on Page 497. If you want these traps suppressed, select **Disabled**.

Site Information Viewable to Guest Users

Operators can enable or disable site information from appearing when a user is in GUEST account mode.

Site Name

Specify a string to associate with the physical module. This parameter is written into the *sysName* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Contact

Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Location

Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

The SNMP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Security Tab of the BHM

An example of the Security tab in a BHM is displayed in Figure 106.

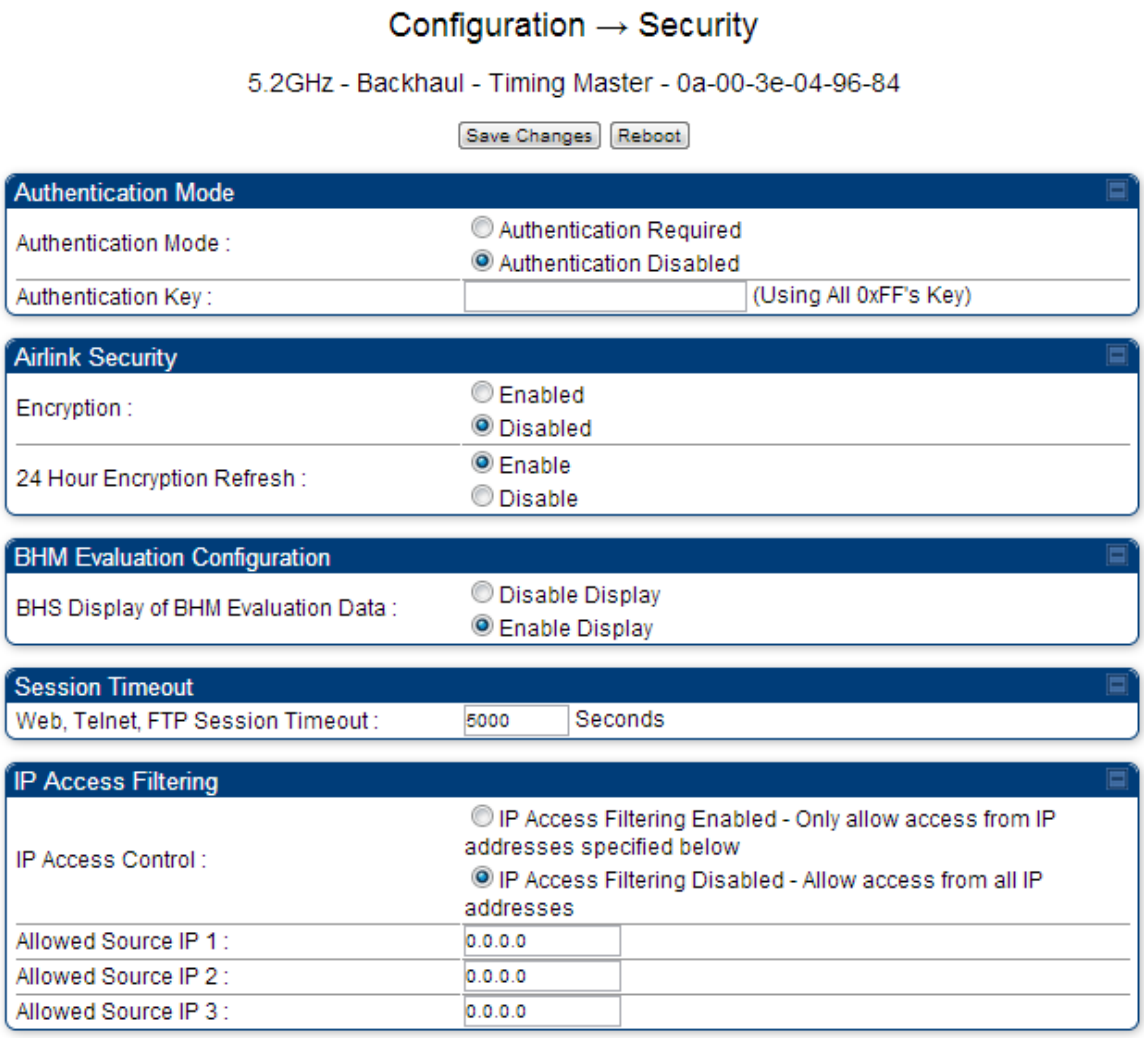


Figure 106: Security tab of BHM, example

In the Security tab of the BHM, you may set the following parameters.

Authentication Mode

Specify whether the BHM should require the BHS to authenticate.

Authentication Key

Only if you set the BHM in the previous parameter to require authentication, specify the key that the BHS should use when authenticating.

Encryption

Specify the type of air link security to apply to this BHM:

- **Encryption Disabled** provides no encryption on the air link. This is the default mode.
- **Encryption Enabled** provides encryption, using a factory-programmed secret key that is unique for each module.

NOTE:
In any BH link where encryption is enabled, the BHS briefly drops registration and re-registers in the BHM every 24 hours to change the encryption key.

24 Hour Encryption Refresh

A BHM that has encryption enabled forces its BHS to re-register once every 24 hours, during which the BHM refreshes the encryption key. This provides a level of security, but results in a brief but daily downtime. Since the refresh occurs in 24 hour increments that begin when the link is established, the only way to set a favorable the time of day (for example, 2:00 AM) for the key refresh is to reboot either the BHM or BHS at the favorable time.

When this feature is disabled, the key is refreshed upon only other re-registration events, such as a reboot. The default status of this feature is **Enable**.

The algorithm used in Advanced Encryption Standard (AES) encryption-capable radios is certified by the National Institute of Standards and Technology (NIST) to meet government Federal Information Processing Standard-197 (FIPS-197) for ensuring secure data communication. Refreshing the key at 24-hour intervals is not needed for AES radios to meet FIPS 197, but provides an level of security above the algorithm itself.

BHS Display of BHM Evaluation Data

You can use this field to suppress the display of data (**Disable Display**) about this BHM on the BHM Evaluation tab of the Tools page in the BHS.

Web, Telnet, FTP Session Timeout

Enter the expiry in seconds for remote management sessions via HTTP, telnet, or ftp access to the BHM.

IP Access Control

You can permit access to the BHM from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address, including access and management by Prizm.

Allowed Source IP *1 to 3*

If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the BHM from any IP address. You may populate as many as all three.

If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.

The Security tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

VLAN tab of the BHM

An example of the VLAN tab in a BHM is displayed in Figure 107.

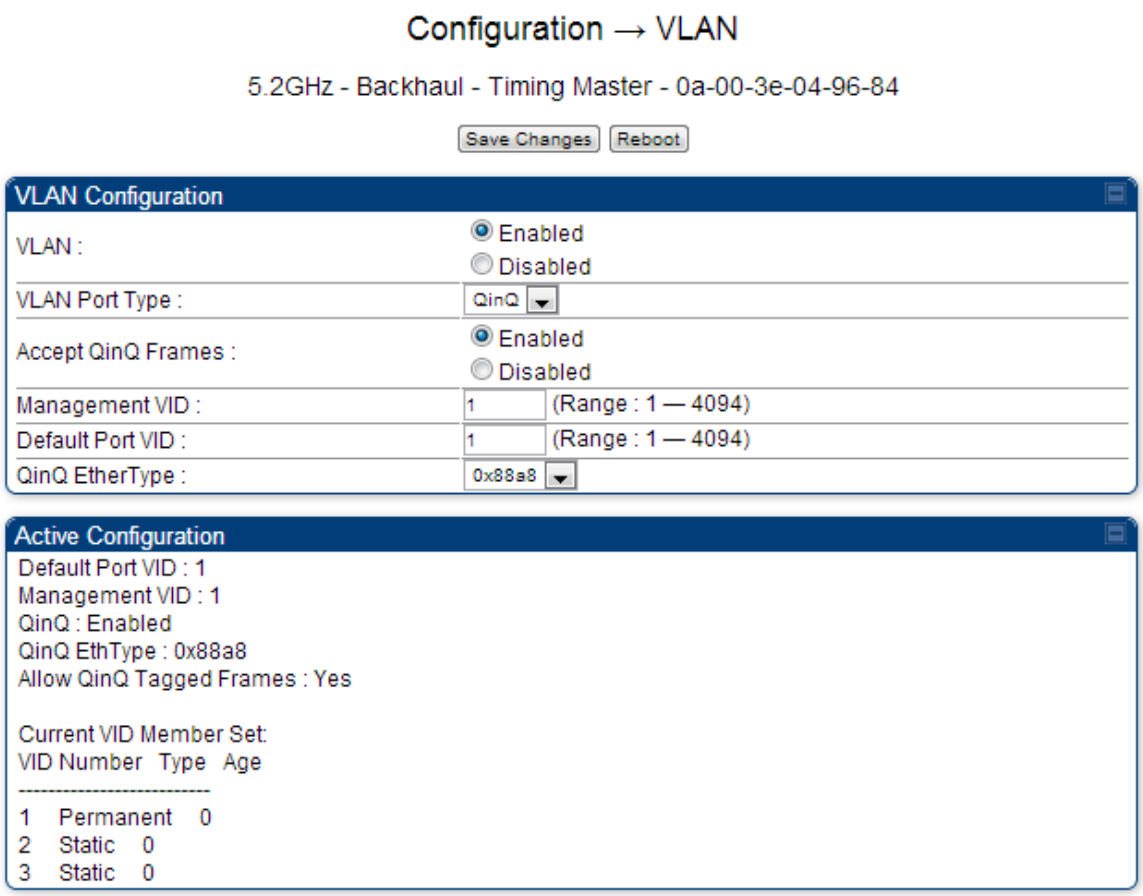


Figure 107: VLAN tab of BHM, example

In the VLAN tab of the BHM, you may set the following parameters.

VLAN

Set the **VLAN** feature to **Enabled** or **Disabled**. When the feature is disabled, the text box for the following parameter is inactive. When the **Management VID** is enabled by this parameter, the module is manageable through only packets that are tagged with the VID configured in that parameter. These parameters have no bearing on tagging in non-management traffic.

By default, **VLAN** is **Enabled** in backhaul modules. With this feature enabled, the backhaul becomes a permanent member of any VLAN VID that it reads in packets that it receives. When the backhaul reboots, it loses these memberships, but begins again to freely adopt memberships in the VIDs that will be permanent until the next reboot.

VLAN Port Type

By default this will be simply **Q**, indicating that it is to operate in the existing manner. The other option is **Q-in-Q**, which indicates that it should be adding and removing the S-Tag, and adding a C-Tag if necessary for untagged packets. The VLAN Port type corresponds to the Ethernet port of the BHS. Currently, the internal management interfaces will always operate as Q ports**.**

Accept QinQ Frames

This option is valid for the Q-in-Q port so that the user may force blocking of existing 802.1ad Q-in-Q frames. This way, only untagged or single tagged packets will come in and out of the Ethernet interface. If a Q-in-Q frame is about ingress or egress the Ethernet interface and this is disabled, it will be dropped and a filter entry will show up on the VLAN Statistics page as DVLAN Egress or DVLAN Ingress.

Management VID

Enter the VID that the operator wishes to use to communicate with the module manager. The range of values is 1 to 4094. The default value is **1**. This text box is inactive if VLAN is set to **Disabled**. In the Cambium fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

Default Port VID

If an untagged packet arrives at the BHM with a **Port VID** configured, when that packet egresses the other end of the backhaul link it will be an 802.1Q tagged packet whose VID is equal to the **Port VID** of the device from where the packet entered the backhaul pair.

As is the case with PMP VLAN, a VID of 1 is a special case VLAN which means that an untagged packet coming into a backhaul unit with a **Port VID** of 1 will exit the other side of the backhaul link untagged. Also if a tagged packet containing a VID equal to the **Port VID** is about to exit the Ethernet port of the backhaul module , that tag will be removed and the packet will be sent untagged.

QinQ EtherType

This parameter is the outer S-VLAN Ethertype that may be configured to interoperate with other networks that use a different Ethertype than the default.

Active Configuration

The Active Configuration block provides the following details as read-only information in this tab.

Default Port VID

This is the value of the parameter of the same name, configured above.

Management VID

In a backhaul module, this value will always be 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

QinQ

This is set to Enabled if VLAN Port Type is set to QinQ, and is set to Disabled if VLAN Port Type is set to Q.

QinQ EthType

This is the value of the QinQ EtherType configured in the AP.

Type

In a backhaul module, this value will always be Permanent, reflective of the fact that the backhaul is not capable of deleting any VID membership, regardless of whether it was learned or set.

Age

In a backhaul module, this value will always be 0, reflective of the fact that the backhaul is not capable of deleting any VID membership, regardless of whether it was learned or set.

The VLAN tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

DiffServ Tab of the BHM

An example of the Diffserv tab in a BHM is displayed in Figure 108.

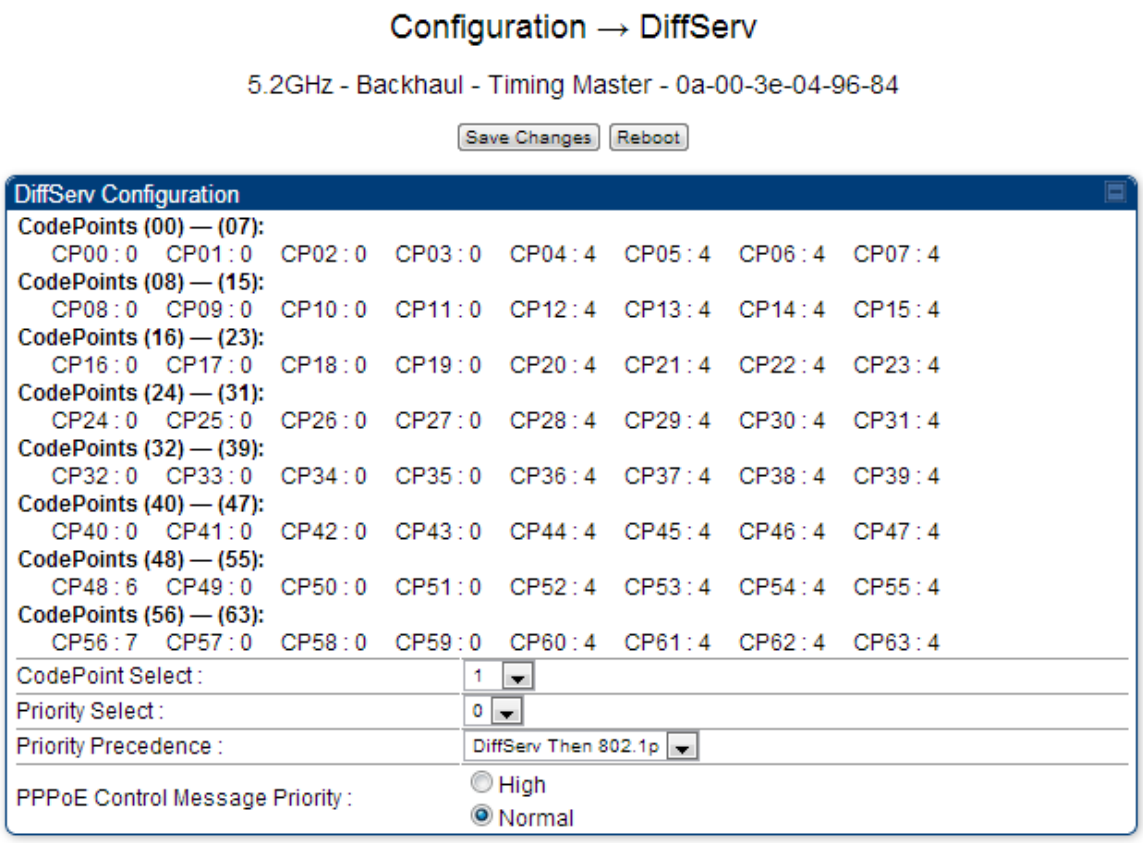

Configuration → DiffServ
5.2GHz - Backhaul - Timing Master - 0a-00-3e-04-96-84
Save Changes
Reboot
DiffServ Configuration
CodePoints (00) — (07):
CP00 : 0 CP01 : 0 CP02 : 0 CP03 : 0 CP04 : 4 CP05 : 4 CP06 : 4 CP07 : 4
CodePoints (08) — (15):
CP08 : 0 CP09 : 0 CP10 : 0 CP11 : 0 CP12 : 4 CP13 : 4 CP14 : 4 CP15 : 4
CodePoints (16) — (23):
CP16 : 0 CP17 : 0 CP18 : 0 CP19 : 0 CP20 : 4 CP21 : 4 CP22 : 4 CP23 : 4
CodePoints (24) — (31):
CP24 : 0 CP25 : 0 CP26 : 0 CP27 : 0 CP28 : 4 CP29 : 4 CP30 : 4 CP31 : 4
CodePoints (32) — (39):
CP32 : 0 CP33 : 0 CP34 : 0 CP35 : 0 CP36 : 4 CP37 : 4 CP38 : 4 CP39 : 4
CodePoints (40) — (47):
CP40 : 0 CP41 : 0 CP42 : 0 CP43 : 0 CP44 : 4 CP45 : 4 CP46 : 4 CP47 : 4
CodePoints (48) — (55):
CP48 : 6 CP49 : 0 CP50 : 0 CP51 : 0 CP52 : 4 CP53 : 4 CP54 : 4 CP55 : 4
CodePoints (56) — (63):
CP56 : 7 CP57 : 0 CP58 : 0 CP59 : 0 CP60 : 4 CP61 : 4 CP62 : 4 CP63 : 4
CodePoint Select :
1
Priority Select :
0
Priority Precedence :
DiffServ Then 802.1p
PPPoE Control Message Priority :
High
Normal

Figure 108: Diffserv tab of BHM, example

In the Diffserv tab of the BHM, you may set the following parameters.

CodePoint 1 through CodePoint 47

CodePoint 49 through CodePoint 55

CodePoint 57 through CodePoint 63

The default priority value for each settable CodePoint is shown in Figure 118. Priorities of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities.

Consistent with RFC 2474

- **CodePoint 0** is predefined to a fixed priority value of **0** (low-priority channel).
- **CodePoint 48** is predefined to a fixed priority value of **6** (high-priority channel).
- **CodePoint 56** is predefined to a fixed priority value of **7** (high-priority channel).

You cannot change any of these three fixed priority values. Among the settable parameters, the priority values (and therefore the handling of packets in the high- or low-priority channel) are set in the AP for all downlinks within the sector and in the SM for each uplink. See DSCP Field on Page 87.

CodePoint Select

This represents the CodePoint Selection to be modified via Priority Select

Priority Select

The priority setting input for the CodePoint selected in CodePoint Select

Priority Precedence

Allows operator to decide if 802.1p or DiffServ priority bits should be used first when making priority decisions.

PPPoE Control Message Priorty

Operators may configure the device to utilize the high priority channel for PPPoE control messages. Configuring the device in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the device.

The Diffserv tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Protocol Filtering Tab of the BHM

An example of the Protocol Filtering tab in a BHM is displayed in Figure 98.

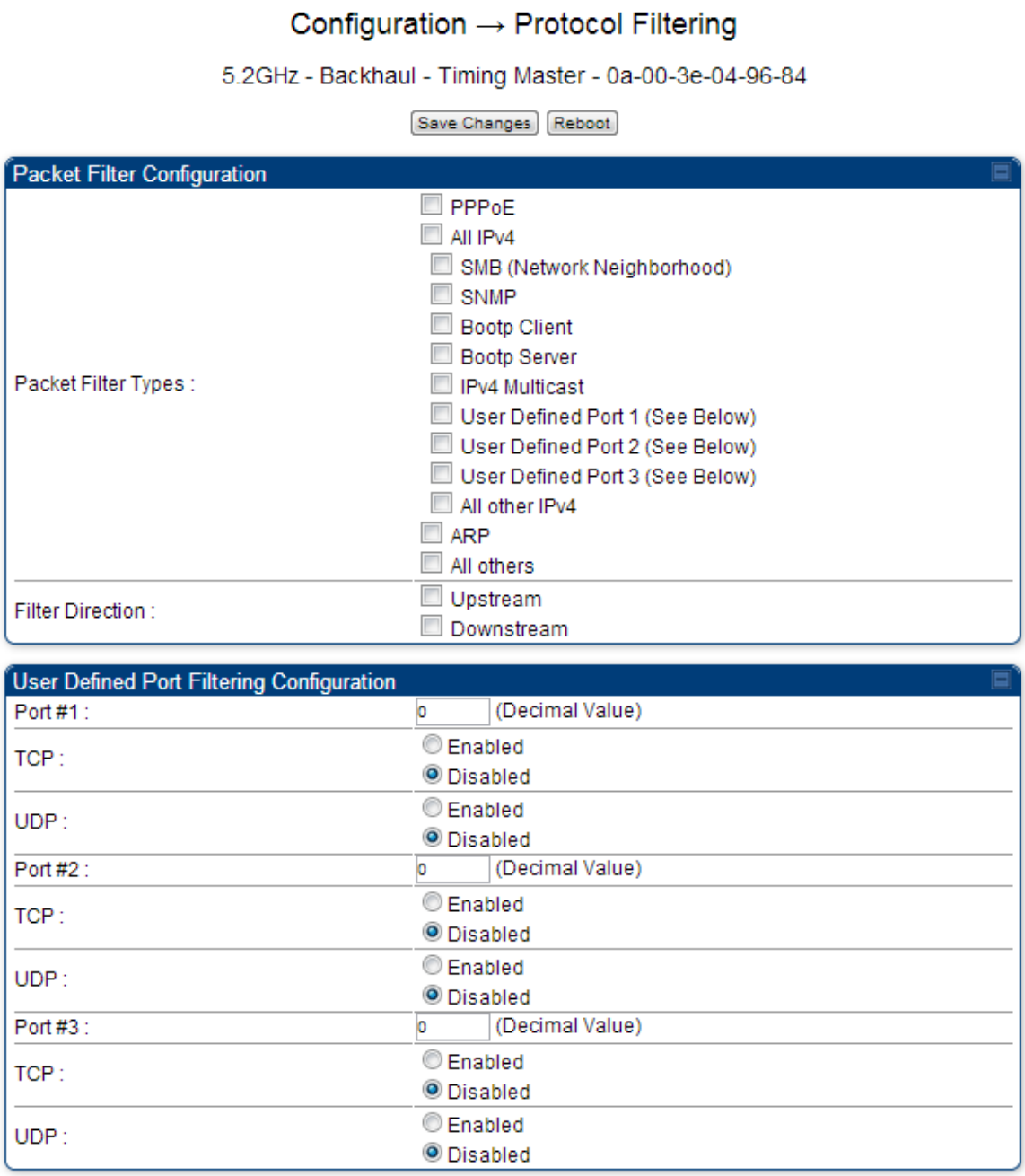


Figure 109: Protocol Filtering tab of SM, example

In the Protocol Filtering tab of the BHM, you may set the following parameters.

Packet Filter Types

For any box selected, the Protocol and Port Filtering feature blocks the associated protocol type. Examples are provided in Protocol and Port Filtering with NAT Disabled on Page 436.

To filter packets in any of the user-defined ports, you must do all of the following:

- Check the box for User Defined Port *n* (See Below) in the Packet Filter Types section of this tab.
- In the User Defined Port Filtering Configuration section of this tab, both
  - provide a port number at **Port #*n***.
  - check **TCP**, **UDP**, or both.

If the **DHCP state** parameter is set to **Enabled** in the Configuration => IP tab of the BHM, *do not* check the **Bootp Client** option for **Packet Filter Types** in its Protocol Filtering tab, because doing so would block the DHCP request. (Filters apply to all packets that leave the BHM via its RF interface, including those that the BHM itself generates.) If you want to keep DHCP enabled and avoid the blocking scenario, select the **Bootp Server** option instead. This will result in responses being appropriately filtered and discarded.

Filter Direction

Select which direction of traffic should be filtered – Upstream (uplink) or Downstream (downlink).

User Defined Port Filtering Configuration

You can specify ports for which to block subscriber access, regardless of whether NAT is enabled. For more information, see Filtering Protocols and Ports on Page 435.

Unit Settings Tab of the BHM

An example of the Unit Settings tab of the BHM is displayed in Figure 110.

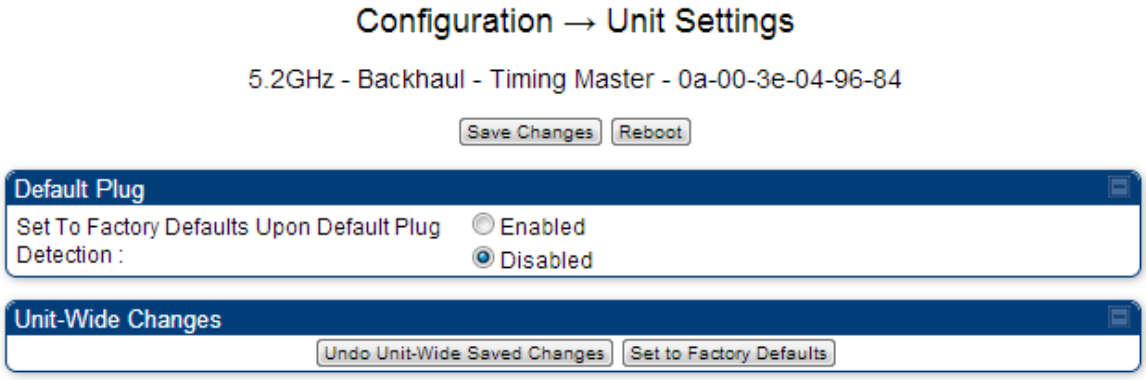


Figure 110: Unit Settings tab of BHM, example

The Unit Settings tab of the BHM contains an option for how the BHM should react when it detects a connected override plug. You may set this option as follows.

Set to Factory Defaults Upon Default Plug Detection

If **Enabled** is checked, then an override/default plug functions as a default plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all parameter values are reset to defaults. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *cannot* see or learn the settings that were previously configured in it. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the default values for any that were not.

If **Disabled** is checked, then an override/default plug functions as an override plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all previously configured parameter values remain and are displayed. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *can* see and learn the settings. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the previous values for any that were not.

See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 433.

The Unit Settings tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Configuring a BH Timing Slave for the Destination

If an ADMINISTRATOR-level password has been set in the BHS, you must log into the module before you can configure its parameters. See Managing Module Access by Passwords on Page 430.

General Tab of the BHS

An example of the General tab in a BHS is displayed in Figure 111.

Figure 111: General tab of BHS, example

In the General tab of the BHS, you may set the following parameters.

Timing Mode

Select **Timing Slave**. This BH will receive sync from another source. Whenever you toggle this parameter to Timing Slave from Timing Master, you should also do the following:

1. Make no other changes in this or any other interface page.
2. Save this change of timing mode.
3. Reboot the BH.

RESULT: The set of interface web pages that is unique to a BHS is made available.

NOTE:
In a BHS that cannot be converted to a BHM, this parameter is not present.

Link Speeds

Specify the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all APs, BHs, and SMs in the operator network.

Region Code

From the drop-down list, select the region in which the radio is operating.
When the appropriate region is selected in this parameter, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard. For further information on DFS, see Radar Signature Detection and Shutdown on Page 127.

The slave radio automatically inherits the DFS type of the master. This behavior ignores the value of the **Region Code** parameter in the slave, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), you should always set the value that corresponds to the local region.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

Bridge Entry Timeout

Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. Timeout occurs when the BHM encounters no activity with the BHS (whose MAC address is the bridge entry) within the interval that this parameter specifies. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.

This parameter governs the timeout interval, even if a router in the system has a longer timeout interval. The default value of this field is 25 minutes.

CAUTION!
An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.

Bridging Functionality

Select whether you want bridge table filtering active (Enable) or not (Disable) on this BHS. Selecting Disable allows you to use redundant BHs without causing network addressing problems. Through a spanning tree protocol, this reduces the convergence time from 25 minutes to mere seconds. However, you should disable bridge table filtering as only a deliberate part of your overall network design. Otherwise, disabling it allows unwanted traffic across the wireless interface.

Power Up Mode With No 802.3 Link

Specify the default mode in which this BHS will power up when it senses no Ethernet link. Select either

- **Power Up in Aim Mode**—the BHS boots in an aiming mode. When the BHS senses an Ethernet link, this parameter is automatically reset to Power Up in Operational Mode. When the BHS senses no Ethernet link within 15 minutes after power up, the BHS carrier shuts off.
- **Power Up in Operational Mode**—the BHS boots in Operational mode and attempts registration. This is the default selection.

Dynamic Rate Adapt

See 2X Operation on Page 89.

Frame Timing Pulse Gated

If this BHS extends the sync pulse to a BHM or an AP behind it, select either

- **Enable**—If this BHS loses sync, then *do not* propagate a sync pulse to the BHM or AP. This setting prevents interference in the event that the BHS loses sync.

- **Disable**—If this BHS loses sync, then propagate the sync pulse anyway to the BHM or AP.

See Wiring to Extend Network Sync on Page 426.

The General tab also provides the following buttons.

Multicast Destination Address

Using Link Layer Discovery Protocol (LLDP), a module exchanges multicast addresses with the device to which it is wired on the Ethernet interface. Although some switches (CMMmicro, for example) do not pass LLDP addresses upward in the network, a radio can pass it as the value of the **Multicast Destination Address** parameter value in the connected device that has it populated.

In this way, an SM can report to Prizm, for example, the multicast address of a connected remote AP, and thus allow Prizm to discover that AP. To allow this, set the message mode in the remote AP to **LLDP Multicast**. Set this parameter in the BHS to **Broadcast**. The SM will pass this address in broadcast mode, and the CMMmicro will pass the address upward in the network, since it does not discard addresses that it receives in broadcast mode.

Where the AP is not behind another device, the **Broadcast** mode will allow discovery of the AP.

Coordinates

Physical radio location data may be configured via the Latitude, Longitude, and Height fields.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

IP Tab of the BHS

An example of the IP tab in a BHS is displayed in Figure 112.

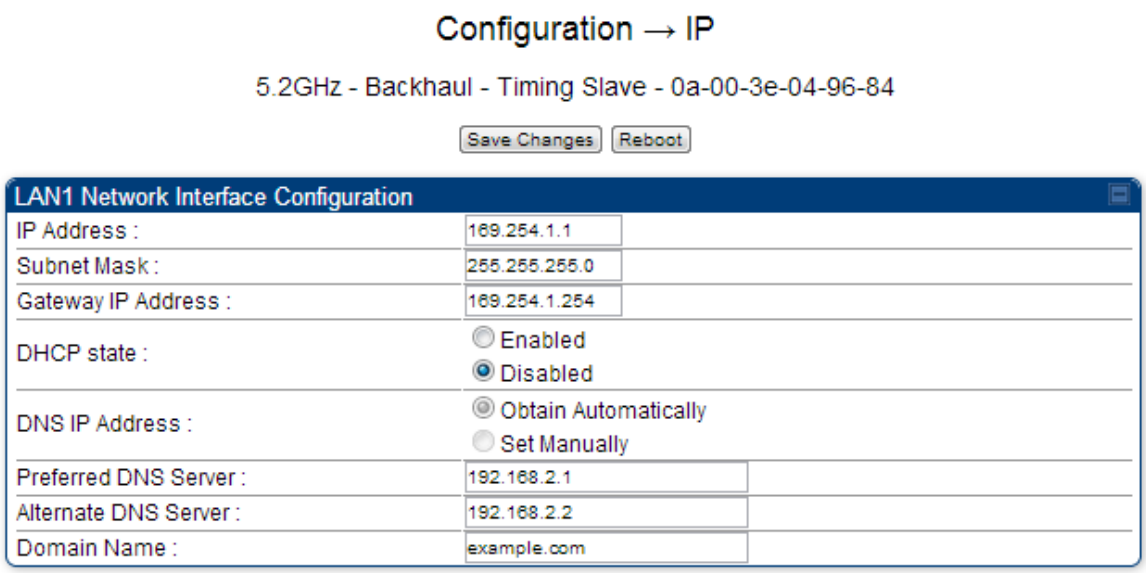


Figure 112: IP tab of BHS, example

In the IP tab of the BHS, you may set the following parameters.

LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to associate with the Ethernet connection on this BHS. (The default IP address from the factory is 169.254.1.1.) If you set and then forget this parameter, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 433.

RECOMMENDATION:
Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the BHS to communicate on the network. The default subnet mask is 255.255.0.0. See Allocating Subnets on Page 164.

LAN1 Network Interface Configuration, Gateway IP Address

Enter the appropriate gateway for the BHS to communicate with the network. The default gateway is 169.254.0.0.

LAN1 Network Interface Configuration, DHCP State

If you select **Enabled**, the DHCP server automatically assigns the IP configuration (IP address, subnet mask, and gateway IP address) and the values of those individual parameters (above) are not used. The setting of this DHCP state parameter is also viewable, but not settable, in the Network Interface tab of the Home page.

LAN1 Network Interface Configuration, DNS IP Address

Canopy devices allow for configuration of a preferred and alternate DNS server IP address either automatically or manually. Devices must set DNS server IP address manually when DHCP is disabled for the management interface of the device. DNS servers may be configured automatically from the DHCP response when DHCP is enabled for the management interface of the device. Optionally devices may be configured to set the DNS server IP address manually when DHCP is enabled for the management interface. The default DNS IP addresses are 0.0.0.0 when configured manually.

LAN1 Network Interface Configuration, Preferred DNS Server

The first address used for DNS resolution.

LAN1 Network Interface Configuration, Alternate DNS Server

Upon failure to reach the Preferred DNS server, the Alternate DNS Server is used.

LAN1 Network Interface Configuration, Domain Name

The operator's management domain name may be configured for DNS. The domain name configuration can be used for configuration of the servers in the operator's network. The default domain name is example.com, and is only used if configured as such.

The IP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the IP Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Radio Tab of the BHS

An example of the Radio tab in a BHS is displayed in Figure 113.

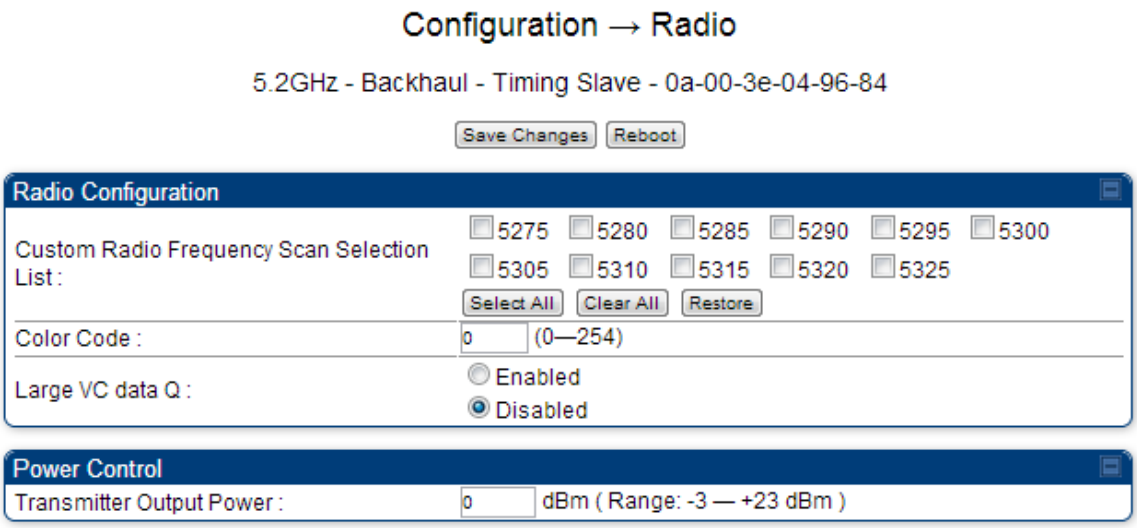


Figure 113: Radio tab of BHS, example

In the Radio tab of the BHS, you may set the following parameters.

Custom Radio Frequency Scan Selection List

Specify the frequency that the BHS should scan to find the BHM. The frequency *band* of the BHs affects what channels you select.

> ***IMPORTANT!***
> In the 2.4-GHz frequency band, the BHS can register to a BHM that transmits on a frequency 2.5 MHz higher than the frequency that the BHS receiver locks when the scan terminates as successful. This establishes a poor-quality link. To prevent this, select frequencies that are at least 5 MHz apart.

In a 2.4-GHz BHS, this parameter displays all available channels, but has only three recommended channels selected by default. See 2.4-GHz AP Cluster Recommended Channels on Page 136.

In a 5.2- or 5.4-GHz BHS, this parameter displays only ISM frequencies. In a 5.7-GHz BHS, this parameter displays both ISM and U-NII frequencies. If you select all frequencies that are listed (default selections), then the module scans for a signal on any channel. If you select only one, then the module limits the scan to that channel. Since the frequencies that this parameter offers for each of these two bands are 5 MHz apart, a scan of *all* channels does not risk establishment of a poor-quality link as in the 2.4-GHz band. Nevertheless, this can risk establishment of a link to the wrong BHM.

A list of channels in the band is provided in Considering Frequency Band Alternatives on Page 134.

(The selection labeled **Factory** requires a special software key file for implementation.)

Color Code

Specify a value from 0 to 254. For registration to occur, the color code of the BHM and the BHS *must* match. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).

RECOMMENDATION:
Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

Large VC data Q

Certain applications such as video Surveillance cameras operate by sending bursts of IP traffic upstream. Some systems will send short bursts of packets at over 50 Mbps and then be idle for some period of time and then send another burst of data.

In order for the RF interface of a radio to accommodate these bursts of traffic, there is a configurable parameter on SM radios as well as BH Master and Slave radios to operate with a large input queue at the radio's data VC. This large queue allows packets which arrive at a rate greater than the radio link capacity to be stored in this deep queue until the radio is ready to transmit them. The queue size has been optimized to allow large packets to be stored just long enough so that there is always data available to be transmitted, but not large enough to cause packets to sit in a queue for a second or more.

Configuration of this parameter is shown on the Configuration => Radio web page on the SM, BHM and BHS. Operators should enable Large VC data Q on the BHM for downlink traffic or enable it on the BHS for uplink traffic.

If an operator is experiencing packet loss in the uplink due to bursting IP traffic and the overalltraffic rate is less than or equal to the uplink capacity of the radio system, then the large VC data Q should be enabled.

For example, a PTP 20 Mbps BH has a video camera connected to the BH Slave (BHS) uplink. To check if packets are being lost at the BHS RF interface the operator should check the "outdiscards Count" at the Statistics->Radio page of the BHS. If this count is incrementing, then packets are being lost at the RF interface of the BHS and the Large VC data Q should be enabled. In the figure below, the outdiscards Count shows 455 discard events since the counter was reset, indicating that probably system performance would be improved by the Large VC data Q.

External Antenna Gain

This parameter applies to connectorized radios (for use with external antenna) only. Using Table 57 as a guide, type in the dB value by which to reduce Dynamic Frequency Selection (DFS) sensitivity to radar signals.

Table 57: Recommended External Antenna Gain values for BHS

Module Type	Recommended Setting
PTP 100 with 9 dB Canopy LENS	9
PTP 100 with standard 18 dB reflector	18
PTP 100 connectorized with 15.5 dBi antenna and 0.5 dB cable loss	15

The value of this parameter does not affect transmitter output power. This parameter is present in only connectorized radios (for usage with an external antenna).

Transmitter Output Power

Nations and regions may regulate transmitter output power. For example

- Connectorized radios require the operator to adjust power based on installed antenna gain to ensure regulatory compliance.
- Legal maximum allowable transmitter output power and EIRP (Equivalent Isotropic Radiated Power) in the 2.4-GHz frequency band varies by country and region. The output power of Series P9 2.4-GHz modules can be adjusted to meet these national or regional regulatory requirements.
- Countries and regions that permit the use of the 5.4-GHz frequency band (CEPT member states, for example), generally require equipment using the band to have adjustable power.

The professional installer of the equipment has the responsibility to

- maintain awareness of applicable regulations.
- calculate the permissible transmitter output power for the module.
- confirm that the initial power setting is compliant with national or regional regulations.

- confirm that the power setting is compliant following any reset of the module to factory defaults.

For information on how to calculate the permissible transmitter output power to enter in this parameter, see Adjusting Transmitter Output Power on Page 382.

The Radio tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

SNMP Tab of the BHS

An example of the SNMP tab in a BHS is displayed in Figure 114.

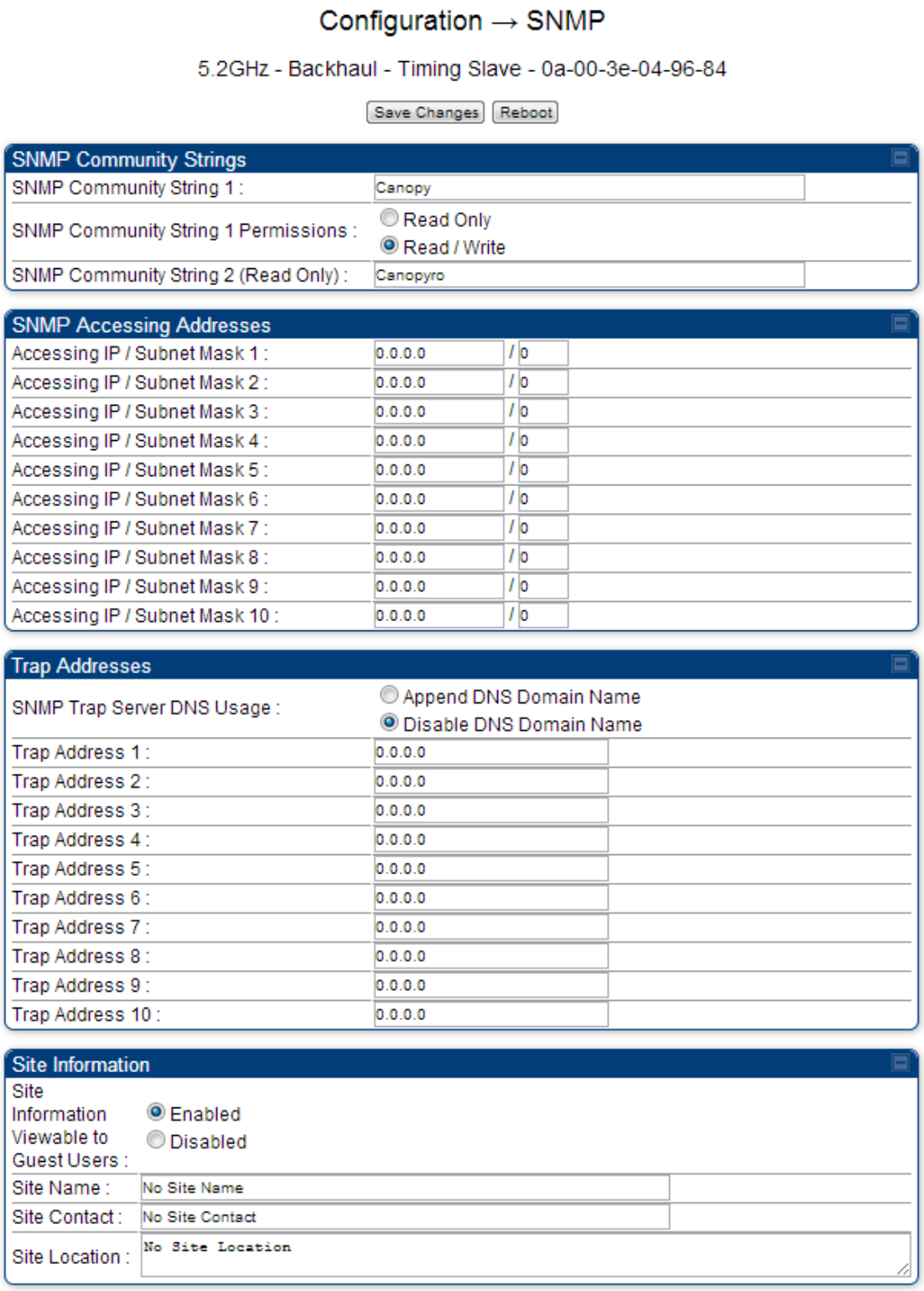

Configuration → SNMP
5.2GHz - Backhaul - Timing Slave - 0a-00-3e-04-96-84
Save Changes
Reboot
SNMP Community Strings
SNMP Community String 1 :
Canopy
SNMP Community String 1 Permissions :
Read Only
Read / Write
SNMP Community String 2 (Read Only) :
Canopyro
SNMP Accessing Addresses
Accessing IP / Subnet Mask 1 :
Accessing IP / Subnet Mask 2 :
Accessing IP / Subnet Mask 3 :
Accessing IP / Subnet Mask 4 :
Accessing IP / Subnet Mask 5 :
Accessing IP / Subnet Mask 6 :
Accessing IP / Subnet Mask 7 :
Accessing IP / Subnet Mask 8 :
Accessing IP / Subnet Mask 9 :
Accessing IP / Subnet Mask 10 :
0.0.0.0 / 0
Trap Addresses
SNMP Trap Server DNS Usage :
Append DNS Domain Name
Disable DNS Domain Name
Trap Address 1 :
Trap Address 2 :
Trap Address 3 :
Trap Address 4 :
Trap Address 5 :
Trap Address 6 :
Trap Address 7 :
Trap Address 8 :
Trap Address 9 :
Trap Address 10 :
0.0.0.0
Site Information
Site Information Viewable to Guest Users :
Enabled
Disabled
Site Name :
No Site Name
Site Contact :
No Site Contact
Site Location :
No Site Location

Figure 114: SNMP tab of BHS, example

In the SNMP tab of the BHS, you may set the following parameters.

SNMP Community String 1

Specify a control string that can allow an Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is **Canopy**.

SNMP Community String 1 Permissions

You can designate the **SNMP Community String 1** to be the password for Prizm, for example, to have read/write access to the module via SNMP, or for all SNMP access to the module to be read only.

SNMP Community String 2 (Read Only)

Specify an additional control string that can allow an Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. The default string is **Canopy2**. This password will never authenticate a user or an NMS to read/write access.

The **Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **Accessing Subnet**, **Trap Address**, and **Permission** parameters.

Accessing IP / Subnet Mask *1 to 10*

Specify the addresses that are allowed to send SNMP requests to this BHS. Prizm or the NMS has an address that is among these addresses (this subnet). You must enter both

- The network IP address in the form xxx.xxx.xxx.xxx
- The CIDR (Classless Interdomain Routing) prefix length in the form /xx

For example

- the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).
- 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the BHS, presuming that the device supplies the correct **Community String** value.

The default treatment is to allow all networks access (set to 0). For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.” You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations.

SNMP Trap Server DNS Usage

The management DNS domain name may be toggled such that the name of the trap server only needs to be specified and the DNS domain name is automatically appended to that name. The default SNMP trap server addresses for all 10 available servers is 0.0.0.0 with the appending of the DNS domain name disabled.

Trap Address *1 to 10*

Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) to which trap information should be sent. Trap information informs Prizm or an NMS that something has occurred. For example, trap information is sent

- after a reboot of the module.
- when Prizm or an NMS attempts to access agent information but either
  - supplied an inappropriate community string or SNMP version number.
  - is associated with a subnet to which access is disallowed.

Site Information Viewable to Guest Users

Operators can enable or disable site information from appearing when a user is in GUEST account mode.

Site Name

Specify a string to associate with the physical module. This parameter is written into the *sysName* SNMP MIB-II object and can be polled by Prizm or an NMS. The buffer size for this field is 128 characters.

Site Contact

Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by Prizm or an NMS. The buffer size for this field is 128 characters.

Site Location

Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by Prizm or an NMS. The buffer size for this field is 128 characters.

The SNMP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Quality of Service (QoS) Tab of the BHS

An example of the Quality of Service tab of the BHS is displayed in Figure 115.

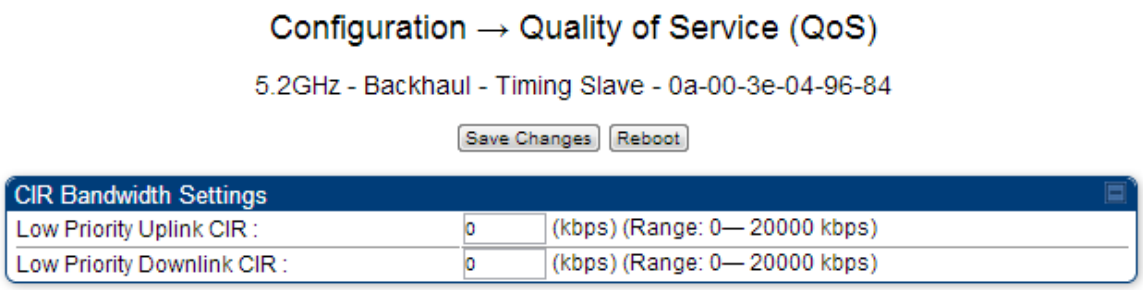


Figure 115: Quality of Service (QoS) tab of BHS, example

In the Quality of Service (QoS) tab of the BHS, you may set the following parameters.

Low Priority Uplink CIR

See

- Committed Information Rate on Page 85
- Setting the Configuration Source on Page 324.

Low Priority Downlink CIR

See

- Committed Information Rate on Page 85
- Setting the Configuration Source on Page 324.

Security Tab of the BHS

An example of the Security tab in a BHS is displayed in Figure 116.

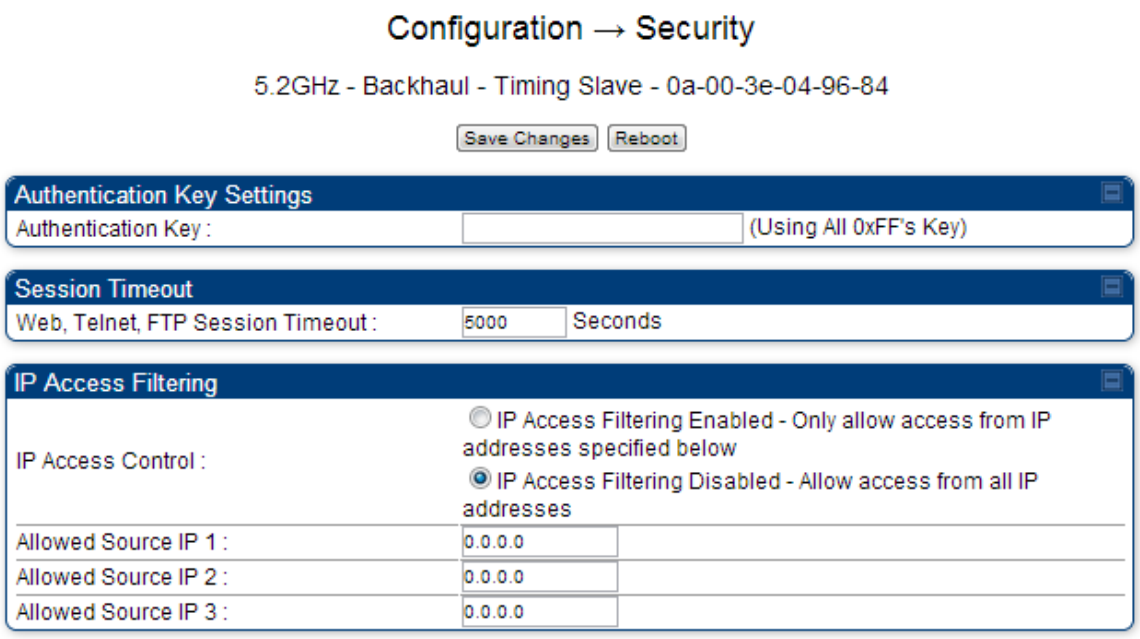

Configuration → Security
5.2GHz - Backhaul - Timing Slave - 0a-00-3e-04-96-84
Save Changes
Reboot
Authentication Key Settings
Authentication Key :
(Using All 0xFF's Key)
Session Timeout
Web, Telnet, FTP Session Timeout :
5000
Seconds
IP Access Filtering
IP Access Control :
IP Access Filtering Enabled - Only allow access from IP addresses specified below
IP Access Filtering Disabled - Allow access from all IP addresses
Allowed Source IP 1 :
0.0.0.0
Allowed Source IP 2 :
0.0.0.0
Allowed Source IP 3 :
0.0.0.0

Figure 116: Security tab of BHS, example

In the Security tab of the BHS, you may set the following parameters.

Authentication Key

Only if the BHM to which this BHS will register requires authentication, specify the key that the BHS should use when authenticating. For alpha characters in this hex key, use only upper case.

NOTE:
Cambium recommends that you enter 32 characters to achieve the maximal security from this feature.

Web, Telnet, FTP Session Timeout

Enter the expiry in seconds for remote management sessions via HTTP, telnet, or ftp access to the BHS.

IP Access Control

You can permit access to the BHS from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address, including access and management by Prizm.

Allowed Source IP *1 to 3*

If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the BHS from any IP address. You may populate as many as all three.

If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.

The Security tab of the BHS also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

VLAN Tab of the BHS

An example of the VLAN tab in a BHS is displayed in Figure 117.

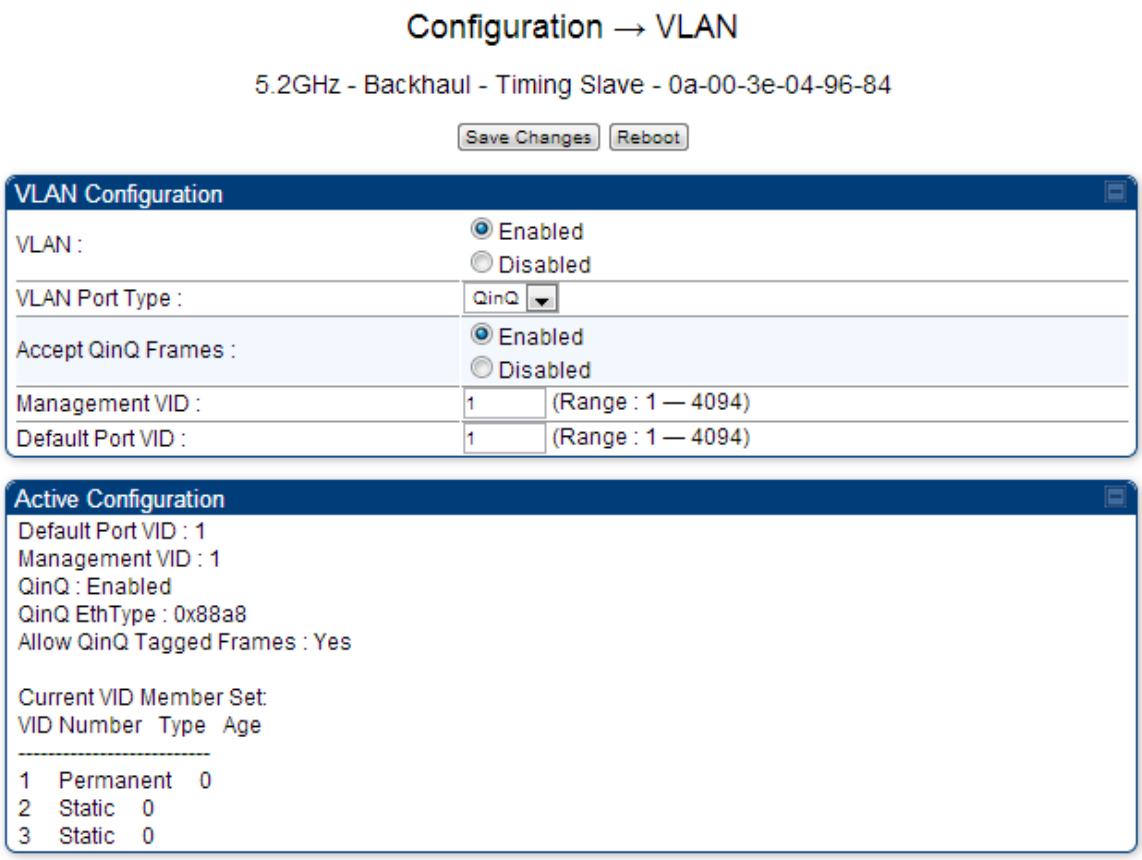


Figure 117: VLAN tab of BHS, example

In the VLAN tab of the BHM, you may set the following parameters.

VLAN

Set the **VLAN** feature to **Enabled** or **Disabled**. When the feature is disabled, the text box for the following parameter is inactive. When the **Management VID** is enabled by this parameter, the module is manageable through only packets that are tagged with the VID configured in that parameter. These parameters have no bearing on tagging in non-management traffic.

By default, **VLAN** is **Enabled** in backhaul modules. With this feature enabled, the backhaul becomes a permanent member of any VLAN VID that it reads in packets that it receives. When the backhaul reboots, it loses these memberships, but begins again to freely adopt memberships in the VIDs that will be permanent until the next reboot.

VLAN Port Type

By default this will be simply Q, indicating that it is to operate in the existing manner. The other option is Q-in-Q, which indicates that it should be adding and removing the S-Tag, and adding a C-Tag if necessary for untagged packets. The VLAN Port type corresponds to the Ethernet port of the BHS. Currently, the internal management interfaces will always operate as Q ports.

Accept QinQ Frames

This option is valid for the Q-in-Q port so that the user may force blocking of existing 802.1ad Q-in-Q frames. This way, only untagged or single tagged packets will come in and out of the Ethernet interface. If a Q-in-Q frame is about ingress or egress the Ethernet interface and this is disabled, it will be dropped and a filter entry will show up on the VLAN Statistics page as DVLAN Egress or DVLAN Ingress.

Management VID

Enter the VID that the operator wishes to use to communicate with the module manager. The range of values is 1 to 4094. The default value is **1**. This text box is inactive if VLAN is set to **Disabled**. In the Cambium fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

Default Port VID

If an untagged packet arrives at the BHM with a **Port VID** configured, when that packet egresses the other end of the backhaul link it will be an 802.1Q tagged packet whose VID is equal to the **Port VID** of the device from where the packet entered the backhaul pair.

As is the case with PMP VLAN, a VID of 1 is a special case VLAN which means that an untagged packet coming into a backhaul unit with a **Port VID** of 1 will exit the other side of the backhaul link untagged. Also if a tagged packet containing a VID equal to the **Port VID** is about to exit the Ethernet port of the backhaul module , that tag will be removed and the packet will be sent untagged.

Active Configuration

The Active Configuration block provides the following details as read-only information in this tab.

Active Configuration Untagged Ingress VID

In a backhaul module, this value will always be 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

Default Port VID

This is the value of the parameter of the same name, configured above.

Management VID

In a backhaul module, this value will always be 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

QinQ

This is set to Enabled if VLAN Port Type is set to QinQ, and is set to Disabled if VLAN Port Type is set to Q.

QinQ EthType

This is the value of the QinQ EtherType configured in the AP.

Type

In a backhaul module, this value will always be Permanent, reflective of the fact that the backhaul is not capable of deleting any VID membership, regardless of whether it was learned or set.

Age

In a backhaul module, this value will always be 0, reflective of the fact that the backhaul is not capable of deleting any VID membership, regardless of whether it was learned or set.

The VLAN tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Diffserv Tab of the BHS

An example of the Diffserv tab in a BHS is displayed in Figure 118.

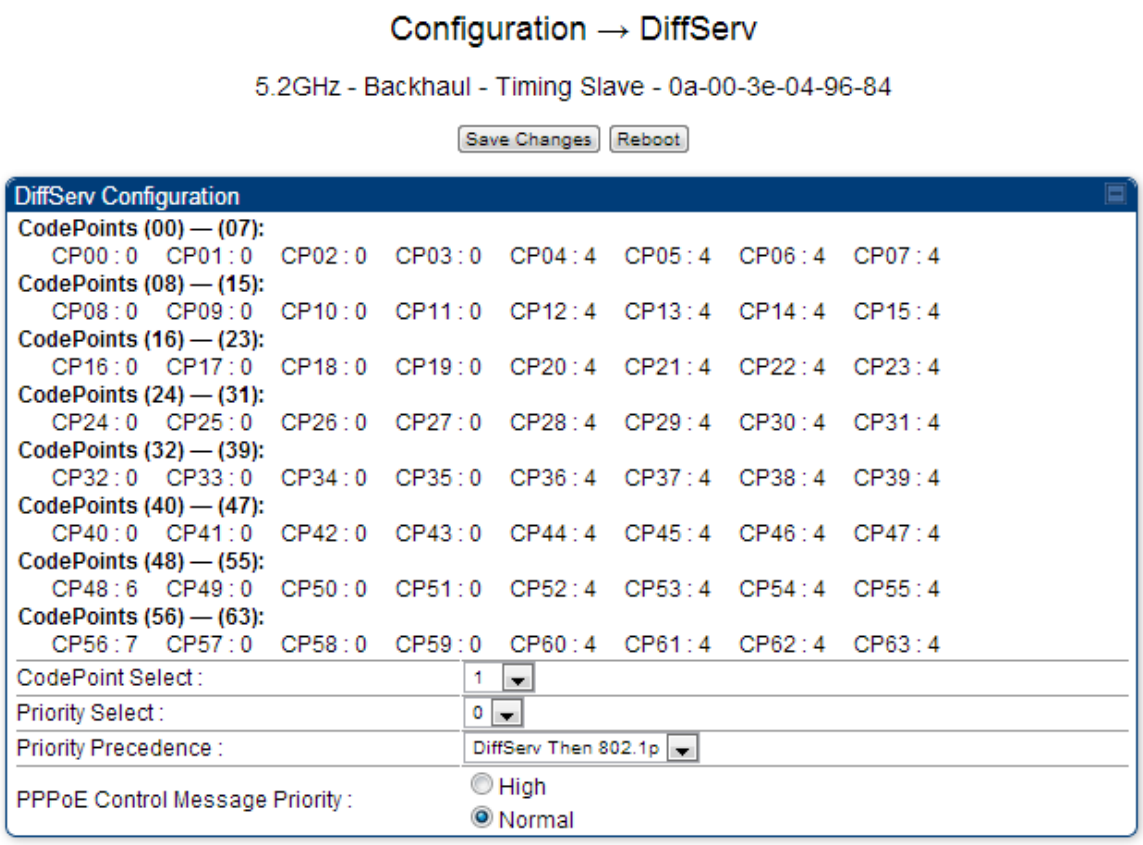

Configuration → DiffServ
5.2GHz - Backhaul - Timing Slave - 0a-00-3e-04-96-84
Save Changes
Reboot
DiffServ Configuration
CodePoints (00) — (07):
CP00 : 0 CP01 : 0 CP02 : 0 CP03 : 0 CP04 : 4 CP05 : 4 CP06 : 4 CP07 : 4
CodePoints (08) — (15):
CP08 : 0 CP09 : 0 CP10 : 0 CP11 : 0 CP12 : 4 CP13 : 4 CP14 : 4 CP15 : 4
CodePoints (16) — (23):
CP16 : 0 CP17 : 0 CP18 : 0 CP19 : 0 CP20 : 4 CP21 : 4 CP22 : 4 CP23 : 4
CodePoints (24) — (31):
CP24 : 0 CP25 : 0 CP26 : 0 CP27 : 0 CP28 : 4 CP29 : 4 CP30 : 4 CP31 : 4
CodePoints (32) — (39):
CP32 : 0 CP33 : 0 CP34 : 0 CP35 : 0 CP36 : 4 CP37 : 4 CP38 : 4 CP39 : 4
CodePoints (40) — (47):
CP40 : 0 CP41 : 0 CP42 : 0 CP43 : 0 CP44 : 4 CP45 : 4 CP46 : 4 CP47 : 4
CodePoints (48) — (55):
CP48 : 6 CP49 : 0 CP50 : 0 CP51 : 0 CP52 : 4 CP53 : 4 CP54 : 4 CP55 : 4
CodePoints (56) — (63):
CP56 : 7 CP57 : 0 CP58 : 0 CP59 : 0 CP60 : 4 CP61 : 4 CP62 : 4 CP63 : 4
CodePoint Select :
1
Priority Select :
0
Priority Precedence :
DiffServ Then 802.1p
PPPoE Control Message Priority :
High
Normal

Figure 118: Diffserv tab of BHS, example

You may set the following Differentiated Services Configuration page parameters.

CodePoint 1 through CodePoint 47

CodePoint 49 through CodePoint 55

CodePoint 57 through CodePoint 63

The default priority value for each settable CodePoint is shown in Figure 118. Priorities of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities.

Consistent with RFC 2474

- **CodePoint 0** is predefined to a fixed priority value of **0** (low-priority channel).
- **CodePoint 48** is predefined to a fixed priority value of **6** (high-priority channel).
- **CodePoint 56** is predefined to a fixed priority value of **7** (high-priority channel).

You cannot change any of these three fixed priority values. Among the settable parameters, the priority values (and therefore the handling of packets in the high- or low-priority channel) are set in the BHM for the downlink and in the BHS for the uplink. See DSCP Field on Page 87.

CodePoint Select

This represents the CodePoint Selection to be modified via Priority Select

Priority Select

The priority setting input for the CodePoint selected in CodePoint Select

Priority Precedence

Allows operator to decide if 802.1p or DiffServ priority bits should be used first when making priority decisions.

PPPoE Control Message Priorty

Operators may configure the BHM to utilize the high priority channel for PPPoE control messages. Configuring the BHM in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network.

Protocol Filtering Tab of the BHS

An example of the Protocol Filtering tab in a BHS is displayed in Figure 98.

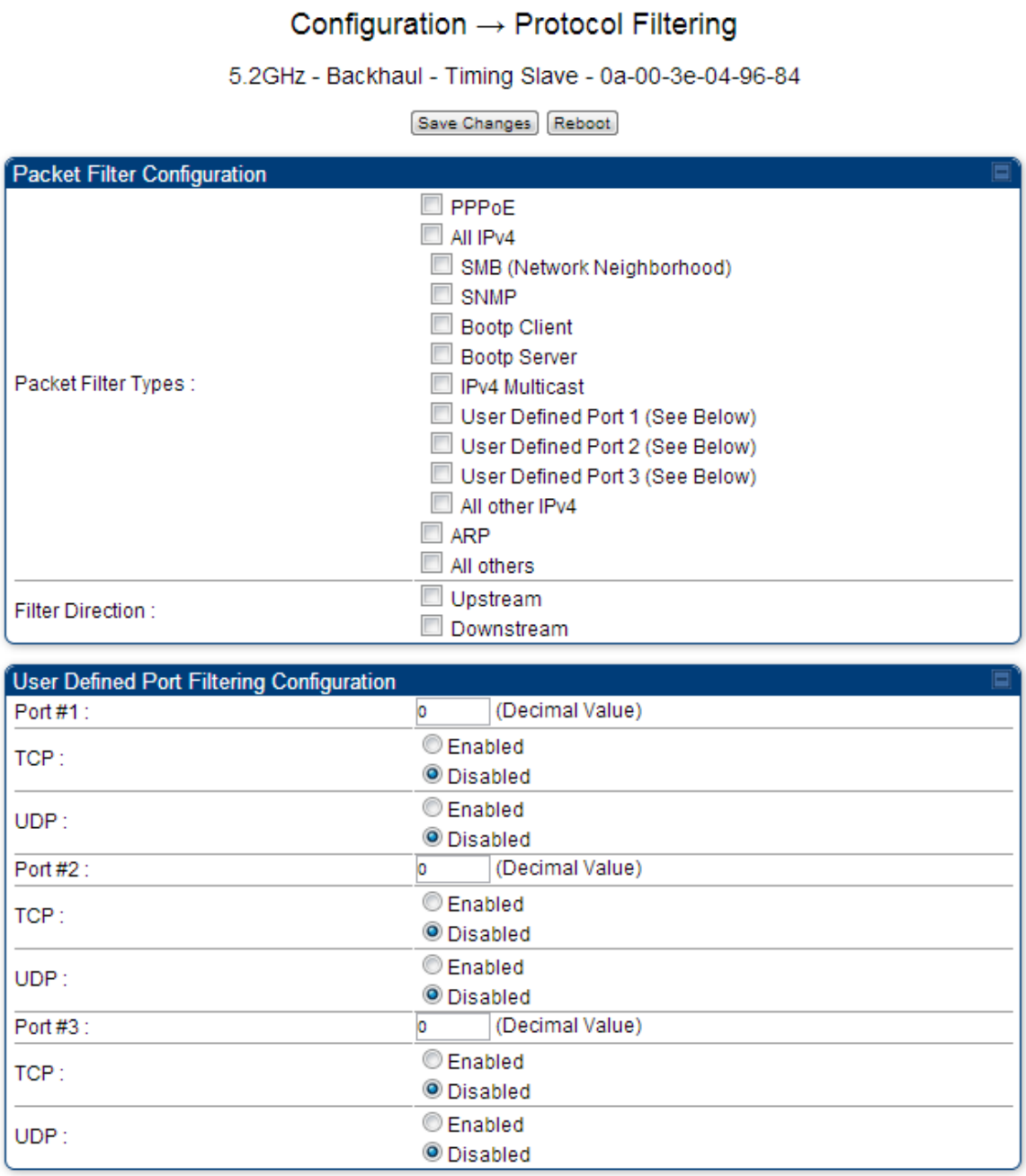


Figure 119: Protocol Filtering tab of SM, example

In the Protocol Filtering tab of the BHS, you may set the following parameters.

Packet Filter Types

For any box selected, the Protocol and Port Filtering feature blocks the associated protocol type. Examples are provided in Protocol and Port Filtering with NAT Disabled on Page 436.

To filter packets in any of the user-defined ports, you must do all of the following:

- Check the box for User Defined Port *n* (See Below) in the Packet Filter Types section of this tab.
- In the User Defined Port Filtering Configuration section of this tab, both
  - provide a port number at **Port #*n***.
  - check **TCP**, **UDP**, or both.

If the **DHCP state** parameter is set to **Enabled** in the Configuration => IP tab of the BHS, *do not* check the **Bootp Client** option for **Packet Filter Types** in its Protocol Filtering tab, because doing so would block the DHCP request. (Filters apply to all packets that leave the BHS via its RF interface, including those that the BHS itself generates.) If you want to keep DHCP enabled and avoid the blocking scenario, select the **Bootp Server** option instead. This will result in responses being appropriately filtered and discarded.

Filter Direction

Select which direction of traffic should be filtered – Upstream (uplink) or Downstream (downlink).

User Defined Port Filtering Configuration

You can specify ports for which to block subscriber access, regardless of whether NAT is enabled. For more information, see Filtering Protocols and Ports on Page 435.

Unit Settings Tab of the BHS

An example of the Unit Settings tab in a BHS is displayed in Figure 120.

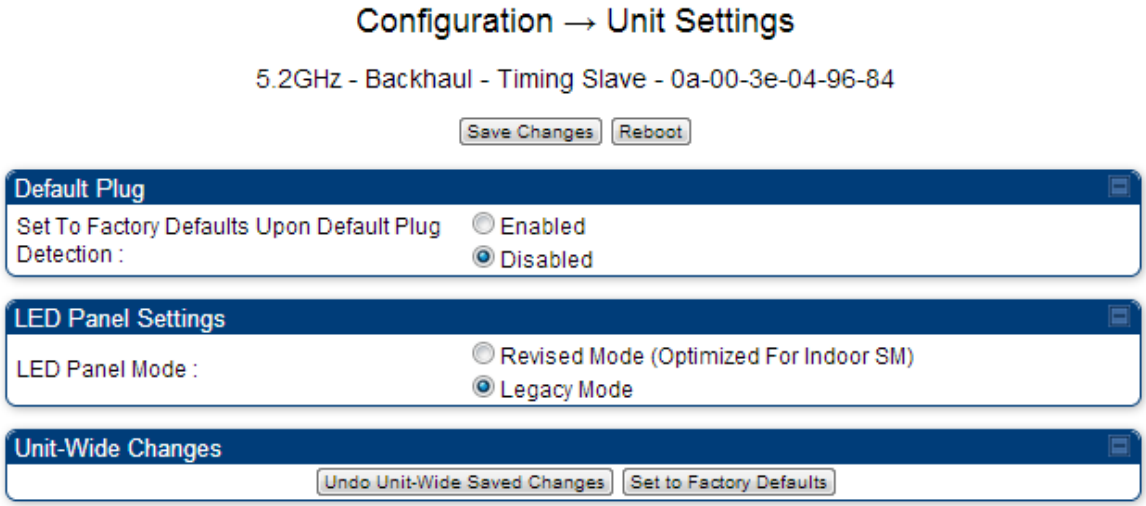


Figure 120: Unit Settings tab of BHS, example

The Unit Settings tab of the BHS contains an option for how the BHS should react when it detects a connected override plug. You may set this option as follows.

Set to Factory Defaults Upon Default Plug Detection

If **Enabled** is checked, then an override/default plug functions as a default plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all parameter values are reset to defaults. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *cannot* see or learn the settings that were previously configured in it. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the default values for any that were not.

If **Disabled** is checked, then an override/default plug functions as an override plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all previously configured parameter values remain and are displayed. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *can* see and learn the settings. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the previous values for any that were not.

See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 433.

LED Panel Mode

Optionally select Revised Mode for simpler use of the LEDs during alignment of the SM. See Diagnostic LEDs on Page 185.

The Unit Settings tab also contains the following buttons.

Undo Unit-Wide Saved Changes

When you click this button, any changes that you made in any tab but did not commit by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all tabs* are reset to the factory settings.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Adjusting Transmitter Output Power

Authorities may require transmitter output power to be adjustable and/or lower than the highest that a module produces. Adjustable power modules include a Radio tab parameter to reduce power on an infinite scale to achieve compliance. If you set this parameter to lower than the supported range extends, the value is automatically reset to the lowest supported value. The high end of the supported range does not vary from radio to radio.

Although transmitter output power is settable in the PMP Series 400 OFDM AP, this AP automatically sets the transmitter output power in its SMs through a feature named Auto-TPC. The conceptual reason for this feature is OFDM reception in the AP is more sensitive to large differences in power levels received from its SMs than is its standard Canopy single-carrier AP counterpart. The OFDM AP sets the SM to the lesser of the following two levels:

- 10 dBm. This is the maximum allowed, because the SM operates with its integrated antenna, and regulation permits EIRP of not greater than 27 dBm.
- power level such that the power that the AP receives from the SM is not greater than 60 dBm.

See also Procedure 3: Reducing transmitter output power on Page 155.

The professional installer of the equipment has the responsibility to

- maintain awareness of applicable regulations.
- calculate the permissible transmitter output power for the module.
- confirm that the initial power setting is compliant.
- confirm that the power setting is compliant following any reset of the module to factory defaults.

The total gain per antenna in 900-MHz and 5.7-GHz radios is stated in Table 58.

Table 58: Total gain per antenna

Module Type	Antenna Gain	Cable Loss[1]	Net Gain
900-MHz Integrated	12.5 dBi	0.2 dB	12 dBi
900-MHz Connectorized[2]	10 to 10.5 dBi	0.3 dB	10 dBi
5.7-GHz Connectorized	settable	0.3 dB + from any additional cable	See Note 3

NOTES:

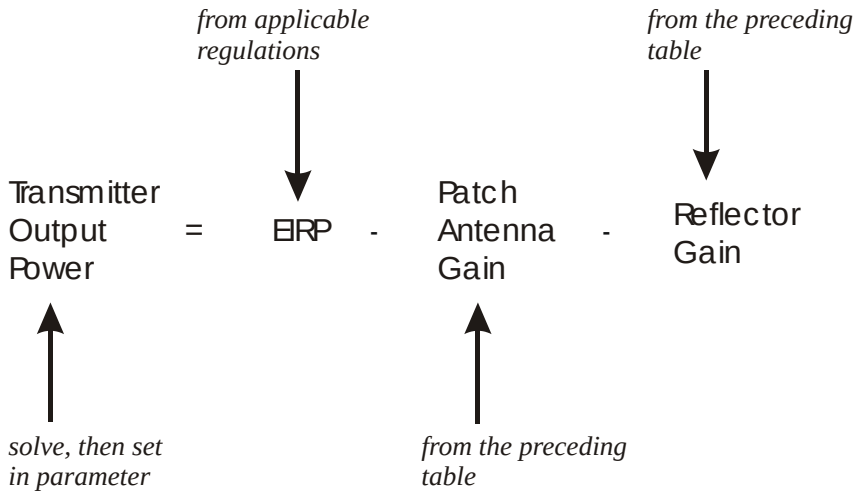
1. Received signal measurements take this loss into account, but the transmitter output power setting cannot. Set the transmitter output power higher by this amount.
2. With Mars, MTI, or Maxrad antenna.
3. Antenna gain minus cable loss.

Integrated patch antenna and reflector gains are provided in Table 59.

Table 59: Patch antenna and reflector gain

Frequency Band Range	Gain	
	Patch Antenna	Reflector
2.4 GHz	8 dBi	11dBi
5.2, 5.4, or 5.7 GHz	7 dBi	18dBi

The calculation of transmitter output power is as follows:



Transmitter output power is settable as dBm on the Radio tab of the module. Example cases of transmitter output power settings are shown in Table 60.

Table 60: Transmitter output power settings, example cases

Frequency Band Range and Antenna Scheme	Region	Maximum EIRP in Region	Transmitter Output Power Setting	
			AP, SM, or BH with No Reflector	SM or BH with Reflector
900-MHz Integrated	U.S.A. Canada	36 dBm (4 W)	24 dBm	
900-MHz Connectorized	U.S.A. Canada	36 dBm (4 W)	26 dBm[1]	
	Australia	30 dBm (1 W)	Depends on antenna	
2.4-GHz Integrated	U.S.A. Canada	Depends on antenna gain	25 dBm	25 dBm
	CEPT states	20 dBm (100 mW)	12 dBm	1 dBm
5.2-GHz Integrated	U.S.A. Canada	30 dBm (1 W)	23 dBm	
5.4-GHz FSK Integrated	CEPT states	30 dBm (1 W)	23 dBm	5 dBm
5.4-GHz OFDM Integrated	U.S.A. Canada Europe	27 dBm (600 mW)	−30 to 10 dBm[2]	
5.4-GHz OFDM Connectorized	U.S.A. Canada Europe	27 dBm (600 mW)	−30 to 15 dBm[2]	
5.7-GHz Connectorized	UK	33 dBm (2 W)	Depends on antenna	Depends on antenna

NOTES:

1. With Mars, MTI, or Maxrad antenna. This is the default setting, and 28 dBm is the highest settable value. The lower default correlates to 36 dBm EIRP where 10-dBi antennas are used. The default setting for this parameter is applied whenever **Set to Factory Defaults** is selected.
2. In a typical case, set the **Transmitter Output Power** parameter in the AP to the maximum allowed. This provides the greatest range for both overall operation and 3X operation. Where full power is not necessary, or where the OFDM network is likely to interfere with a nearby network, incrementally reduce the setting and monitor RF performance.

Chapter 19: Installing Components

RECOMMENDATION:
Use *shielded* cable for all infrastructure connections associated with BHs, APs, and CMMs. The environment that these modules operate in often has significant unknown or varying RF energy. Operator experience consistently indicates that the additional cost of shielded cables is more than compensated by predictable operation and reduced costs for troubleshooting and support.

PDA Access to Modules

For RF spectrum analysis or module aiming on a roof or tower, a personal digital assistant (PDA) is easier to carry than, and as convenient to use as, a notebook computer. The PDA is convenient to use because no scrolling is required to view

- spectrum analysis results.
- RSSI and jitter.
- master module evaluation data.
- information that identifies the module, software, and firmware.

To access this data in a format the fits a 320 x 240 pixel PDA screen, the PDA must have all of the following:

- a Compact Flash card slot.
- any of several Compact Flash wired Ethernet cards.
- a wired Ethernet connection to the module.
- a browser directed to http://*ModuleIPAddress*/pda.html.

Installing an AP

Installing a PMP 100 Series AP

To install a PMP 100 Series (FSK) AP, perform the following steps.

Procedure 17: Installing the FSK AP

1. Begin with the AP in the powered-down state.
2. Choose the best mounting location for your particular application. Modules need not be mounted next to each other. They can be distributed throughout a given site. However, the 60° offset must be maintained. Mounting can be done with stainless steel hose clamps or another equivalent fastener.
3. Align the AP as follows:
   a. Move the module to where the link will be unobstructed by the radio horizon and no objects penetrate the Fresnel zone. (The Canopy System Calculator page AntennaElevationCalcPage.xls automatically calculates the minimum antenna elevation that is required to extend the radio horizon to the other end of the link. The Canopy System Calculator page FresnelZoneCalcPage.xls automatically calculates the Fresnel zone clearance that is required between the visual line of sight and the top of a high-elevation object.)
   b. Use a local map, compass, and/or GPS device as needed to determine the direction that one or more APs require to each cover the intended 60° sector.
   c. Apply the appropriate degree of downward tilt. (The Canopy System Calculator page DowntiltCalcPage.xls automatically calculates the angle of antenna downward tilt that is required.)
   d. Ensure that the nearest and furthest SMs that must register to this AP are within the beam coverage area. (The Canopy System Calculator page BeamwidthRadiiCalcPage.xls automatically calculates the radii of the beam coverage area for PMP 100 Series APs.)
4. Using stainless steel hose clamps or equivalent fasteners, lock the AP in the proper direction and downward tilt.
5. Remove the base cover of the AP. (See Figure 55 on Page 184.)
6. Attach the cables to the AP.
   (See Procedure 5 on Page 190.)

NOTE: When power is applied to a module or the unit is reset on the web-based interface, the module requires approximately 25 seconds to boot. During this interval, self-tests and other diagnostics are being performed. See Table 46 on Page 185.

Installing a PMP 400 Series AP

To install a PMP 400 Series (OFDM) AP, perform the following steps.

Procedure 18: Installing the OFDM AP

1. Inventory the parts to ensure that you have them all before you begin.
   NOTE: The full set of parts is shown in Figure 121.

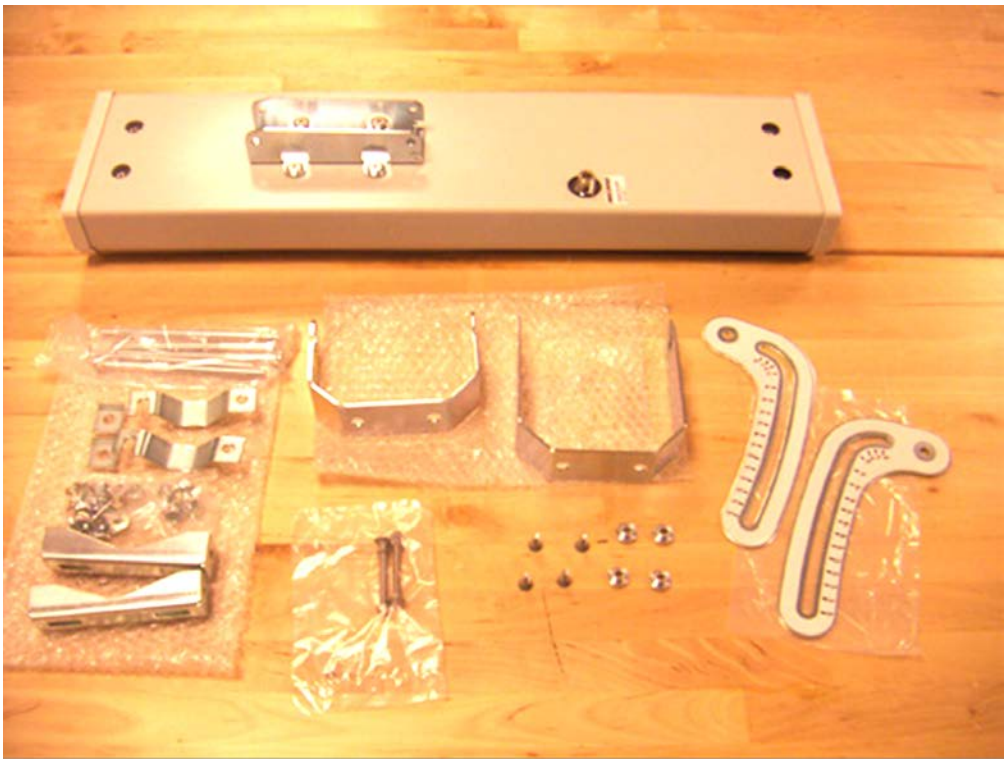


Figure 121: Parts inventory for OFDM AP installation

2. Assemble the upper bracket as shown in Figure 122.

Figure 122: Assembled upper bracket for OFDM AP

3. Connect the AP to its antenna as shown in Figure 123.

Figure 123: OFDM AP connected to its antenna

4. Attach the AP to its antenna as shown in Figure 124.

Figure 124: OFDM AP mounted to its antenna

5. Attach the lower bracket to the antenna as shown in Figure 124 above.
6. Use a local map, compass, and/or GPS device as needed to determine the direction that one or more APs require to each cover the 90° sector.
7. Ensure that the nearest and furthest SMs that must register to this AP are within the 3-dB beam pattern of 60° azimuth by 5° elevation with near-in null fill coverage.
8. Choose the best mounting location for your particular application.
   NOTE: Use the embedded spectrum analyzer or a commercial analyzer to evaluate the frequencies present in various locations. OFDM APs need not be mounted next to each other. They can be distributed throughout a given site. However, the 90° offset must be maintained. If you want to co-locate these APs with PMP 100 Series APs of the 5.4-GHz frequency band range, plan to allow at least 25 MHz of separation between their center channels.
9. Attach the upper bracket to the pole or tower as shown in Figure 125.

Figure 125: OFDM AP ready for tower mount

10. Hang the AP/antenna assembly onto the upper bracket as shown in Figure 126.

Figure 126: Hanging OFDM AP assembly onto upper bracket of pole mount

11. Attach the lower bracket to the pole or tower as shown in Figure 127 and Figure 128.

Figure 127: OFDM AP attached to pole or tower

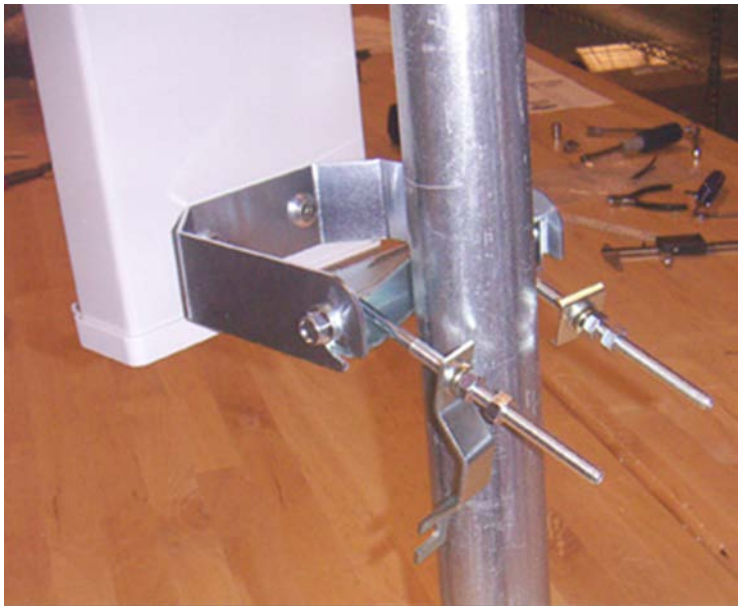


Figure 128: OFDM antenna lower bracket with quick-connect

12. Remove the cover of the 600SS Surge Suppressor.
13. With the cable openings facing downward, mount the 600SS as close as possible to the point where the Ethernet cable will penetrate the residence or building.
14. Using diagonal cutters or long nose pliers, remove the knockouts that cover the cable openings to the 600SS.
15. Connect an Ethernet cable from the power adapter to either RJ-45 port of the 600SS.
16. Remove the bottom cover of the AP.
17. Secure a ground strap to the ground lug (circled in Figure 129) on the bottom of the AP.
18. Secure the ground strap to the pole, tower, or other trusted ground.

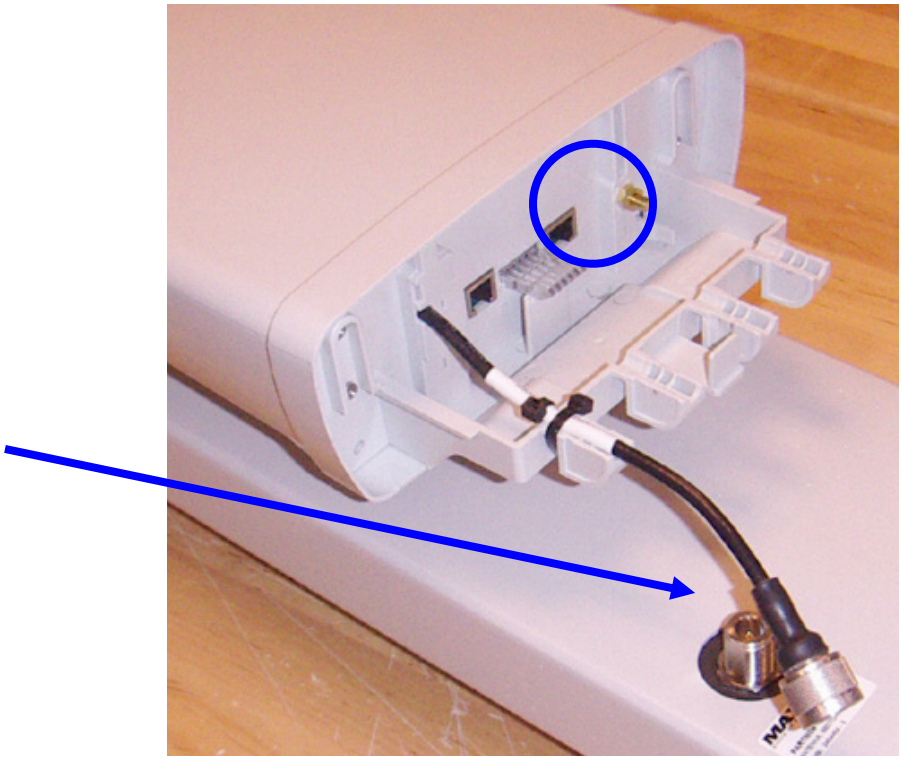


Figure 129: Ground lug and coaxial cable of OFDM AP

19. Connect the Ethernet cable from the AP to the other RJ-45 port of the 600SS.
20. Wrap an AWG 10 (or 6mm^2) copper wire around the Ground post of the 600SS.
21. Tighten the Ground post locking nut in the 600SS onto the copper wire.
22. Securely connect the copper wire to the grounding system (Protective Earth) according to applicable regulations.
23. Replace the cover of the 600SS surge suppressor.
24. Replace the bottom cover of the AP.
25. Adjust the initial down tilt of the AP/antenna assembly to 5°, −3 dB beam elevation, with near-in null fill.
    NOTE: The down tilt bracket is shown in Figure 130.

Figure 130: Down tilt adjustment bracket of OFDM AP

26. Connect the coax cable to the antenna.
27. Weather-seal the connector on the coax cable (identified by arrow in Figure 129 above).

Installing a Connectorized Flat Panel Antenna

To install a connectorized flat panel antenna to a mast or structure, follow instructions that the manufacturer provides. Install the antenna safely and securely, consistent with industry practices.

The Universal Mounting Bracket available from Cambium (Part Number SMMB-1 and consisting of a mounting bracket and L-shaped aluminum tube) holds one module, but cannot hold both the module and a connectorized antenna. The SMMB-2 is a heavy duty bracket that can hold both a 900-MHz or 5.7-GHz connectorized module and its connectorized antenna. See Module Support Brackets on Page 57.

IMPORTANT!
Connectorized antennas *require* professional installation.

The professional installer is responsible for

- selection of an antenna that the regulatory agency has approved for use with the CAP 9130 AP and CAP 9130 SM.
- setting of the gain consistent with regulatory limitations and antenna specifications.
- ensuring that the polarity—horizontal or vertical—is identical on both ends of the link. (This may be less obvious where an integrated antenna is used on one end and a connectorized on the other.)
- use of moisture sealing tape or wrap to provide long-term integrity for the connection.

Although a vertically polarized signal propagates better than a horizontally polarized signal (because of the magnetic field of the earth), vertical polarization is typically better for long distance only where noise above the thermal noise floor is negligible. In some applications, cross polarization may improve signal separation, but typically to only 9 dB of separation at 900 MHz and 15 to 20 dB in the 5.*n*-GHz frequency band ranges.

Weatherproofing a 900 MHz Connectorized Antenna

To prevent moisture from ingressing the rear of the antenna, following the procedure below:

Procedure 19: Weatherproofing the 900 MHz connectorized antenna

1. Using an elastomeric polyurethane-based coating (such as a spray-on truck bed liner), cover each of the plastic standoffs located on the rear of the antenna.

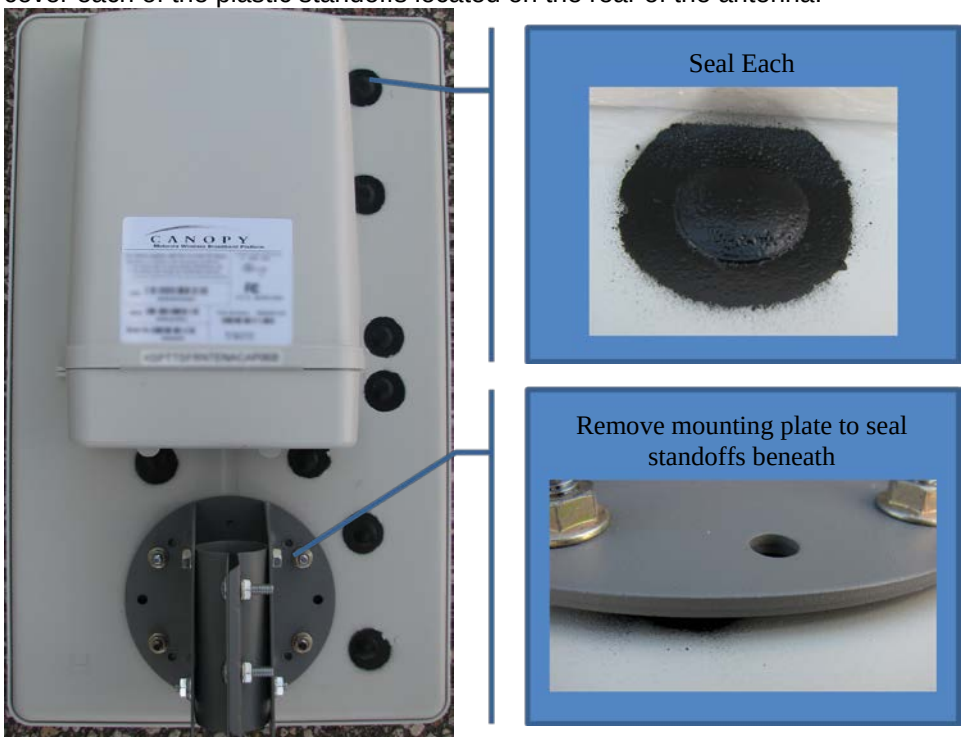


Figure 131: Sealing 900MHz antenna standoffs

2. Using a silicone caulking, seal the gap between the radio and antenna.

Figure 132 Sealing between the 900MHz radio and antenna

Installing a GPS Antenna

For instructions on GPS antenna installation, see the user guide that is dedicated to the CMM/UGPS products.

Installing a Cluster Management Module

For instructions on CMM2 (Cluster Management Module 2), CMM3 (CMMmicro), or CMM4 installation, including the outdoor temperature range in which it is acceptable to install the unit, tools required, mounting and cabling instructions, and connectivity verification, see the user guide that is dedicated to that particular product.

Installing an SM

Configuring the Laptop for Connection to SMs

Windows Laptop

To configure a Windows laptop for connection to SMs for installation, perform the following steps.

Procedure 20: Configuring a Windows laptop

1. Select **Start→Control Panel**.
2. Select **Network and Internet Connections** (or the similarly labeled category).
3. Select
   - **Network Connections**, if your platform is XP.
   - **Manage Network Connections**, if your platform is Vista.
4. Right click on a LAN whose status is shown as Connected and select **Properties** from the drop-down list.
5. Click to highlight **Internet Protocol (TCP/IP)**.
   NOTE An example is shown in Figure 133.

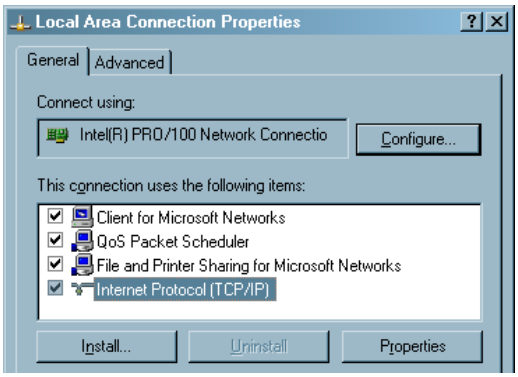


Figure 133: Example Local Area Connection Properties window

6. Click the **Properties** button.
7. In the General tab, select **Use the following IP address**.
   NOTE: An example is shown in Figure 134.

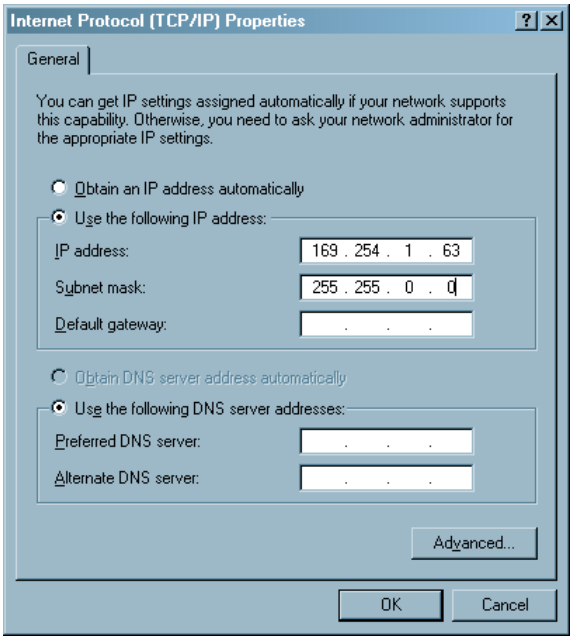

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
169 . 254 . 1 . 63
Subnet mask:
255 . 255 . 0 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 134: Example Internet Protocol (TCP/IP) Properties window

8. For IP address, type in **`169.254.1.63`**.
9. For Subnet mask, type in **`255.255.0.0`**.
10. In the Internet Protocol (TCP/IP) Properties window, click the **OK** button.
11. Click the **Close** button to dismiss the Local Area Connections window.
12. Close the Network Connections window.
    RESULT: The laptop is now configured to reach the interfaces of SMs whose IP addresses are default from the factory. However, the current setting inhibits normal access to the Internet.

13. Whenever you want to access the Internet, reset the General tab to **Obtain an IP address automatically**, but leave the special configuration for the 169 net intact.
14. Whenever you want to use the laptop for SM installations, reset the General tab to **Use the following IP address** and the 169 net.

Linux Laptop

To configure a Linux laptop for connection to SMs for installation, perform the following steps.

Procedure 21: Configuring a Linux laptop

1. On your Linux console, log in as **root**.
2. Enter **ip addr show**.
3. Write down the string that is in the final position of the system response (for example, eth0) to use as the *NIC* in the next step.
4. Enter **ip addr add 169.254.1.63/16 dev *NIC***.
   RESULT: The laptop is now configured to reach the interfaces of SMs whose IP addresses are default from the factory. However, the current setting inhibits normal access to the Internet.
5. Enter **ip addr show**.
   RESULT: The system response confirms the configuration.
6. Whenever you want to access the Internet, perform the following steps:
   a. Log in as **root**.
   b. Enter **netconfig**.
   c. When prompted on whether to set up networking, select **Yes**.
   d. Tab to highlight the **Use Dynamic IP Configuration** option.
   e. Press the spacebar.
      RESULT: The laptop will automatically obtain an IP address and will be able to access the Internet.
7. Whenever you want to use the laptop for SM installations, perform Steps 1 through 5 of this procedure.

Installing a PMP 100 Series SM

Installing a PMP 100 Series SM consists of two procedures:

- Physically installing the SM on a residence or other location and performing a course alignment using the alignment tone (Procedure 22).
- Verifying the AP to SM link and finalizing alignment using review of power level and jitter, link tests, and review of registration and session counts (Procedure 24 on Page 404).

Procedure 22: Installing the FSK SM

1. Choose the best mounting location for the SM.
2. Select the type of mounting hardware appropriate for this location.
   NOTE: For mounting 2.4, 5.2, 5.4, and 5.7 GHz SMs, Cambium offers the SMMB-1 mounting bracket. For mounting 900 MHz SMs, Cambium offers the SMMB-2 mounting bracket.
3. Attach the mounting bracket to the structure.
4. Remove the base cover of the SM. (See Figure 55 on Page 184.)
5. Terminate the UV outside grade Category 5 Ethernet cable with an RJ-45 connector, and connect the cable to the SM. (See Procedure 8 on Page 199.)
6. Wrap a drip loop in the cable.
7. Optionally, attach the SM to the arm of the Passive Reflector dish assembly as shown in Figure 135 or snap a LENS onto the SM.

RECOMMENDATION:
A reflector in this instance reduces the beamwidth to reduce interference. The arm is molded to receive and properly aim the module relative to the aim of the dish. Use stainless steel hose clamps for the attachment.

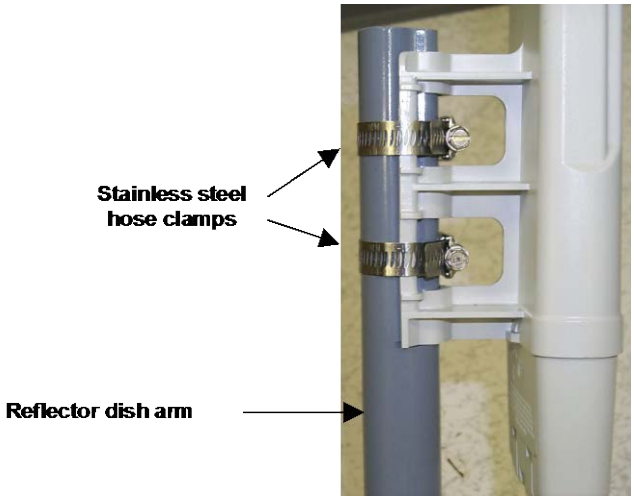


Figure 135: SM attachment to reflector arm

8. Use stainless steel hose clamps or equivalent fasteners to lock the SM into position.
   NOTE: The SM grounding method is shown in Figure 136.

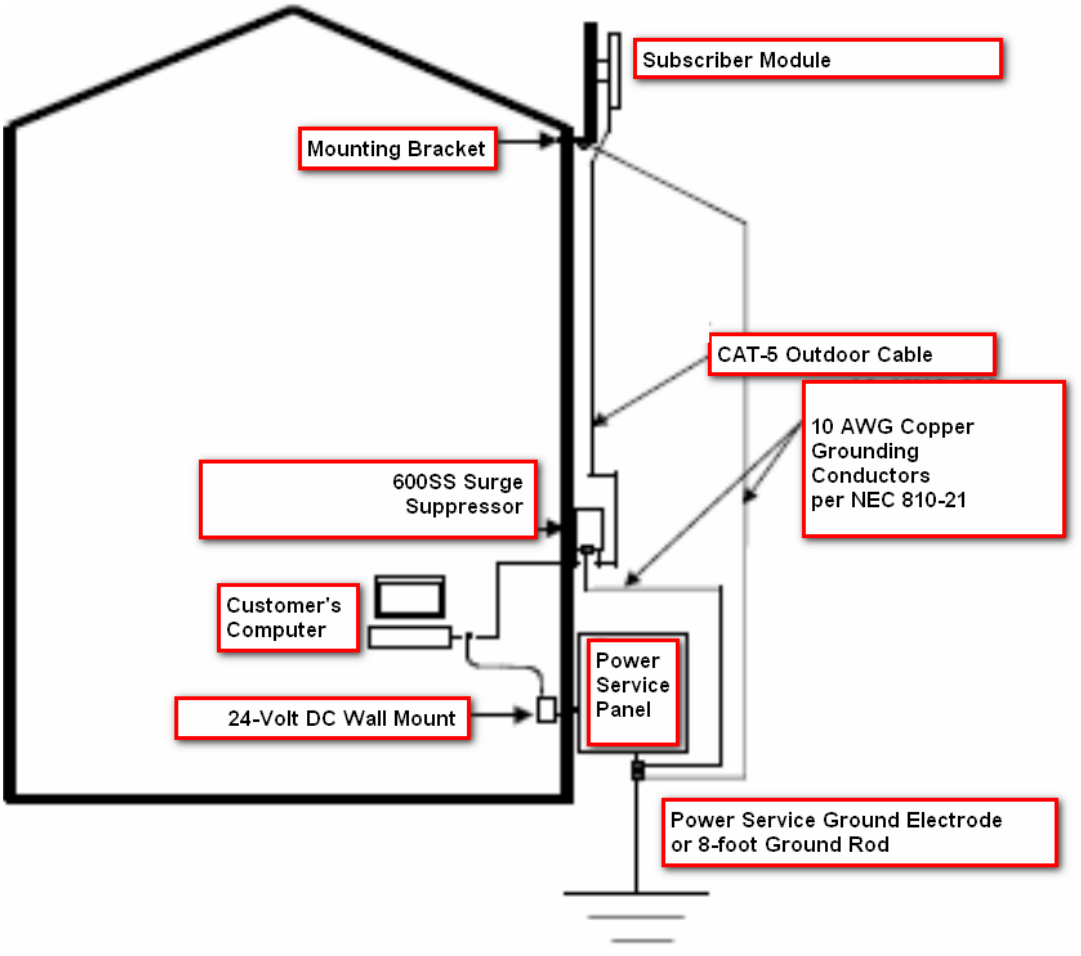
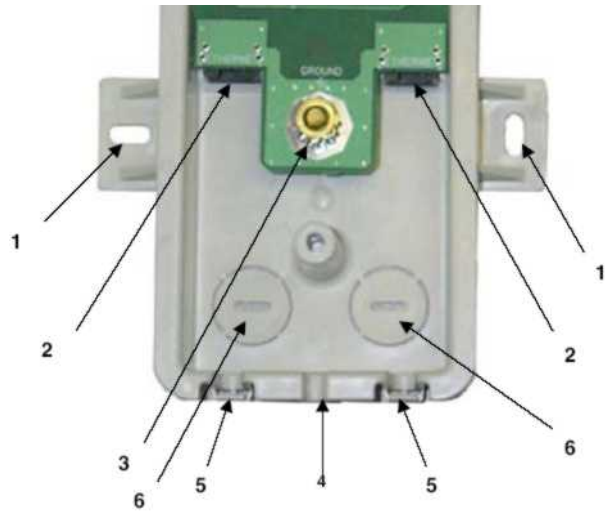


Figure 136: SM grounding per NEC specifications

9. Refer to Grounding SMs on Page 178.
10. Remove the cover of the 600SS Surge Suppressor.
    NOTE: The inside of the surge suppressor is shown in Figure 137.



KEY TO CALLOUTS

1 Holes—for mounting the Surge Suppressor to a flat surface (such as an outside wall). The distance between centers is 4.25 inches (108 mm).

2 RJ-45 connectors—One side (neither side is better than the other for this purpose) connects to the product (AP, SM, BHM, BHS, or cluster management module). The other connects to the AC adaptor's Ethernet connector.

3 Ground post—use heavy gauge (10 AWG or 6 mm^2) copper wire for connection. Refer to local electrical codes for exact specifications.

4 Ground Cable Opening—route the 10 AWG (6 mm^2) ground cable through this opening.

5 CAT-5 Cable Knockouts—route the two CAT-5 cables through these openings, or alternatively through the Conduit Knockouts.

6 Conduit Knockouts—on the back of the case, near the bottom. Available for installations where cable is routed through building conduit.

Figure 137: Internal view of Canopy 600SS Surge Suppressor

11. With the cable openings facing downward, mount the 600SS to the *outside* of the subscriber premises, as close to the point where the Ethernet cable penetrates the residence or building as possible, and as close to the grounding system (Protective Earth) as possible.
12. Wrap an AWG 10 (or 6mm^2) copper wire around the Ground post of the 600SS.
13. Tighten the Ground post locking nut in the 600SS onto the copper wire.
14. Securely connect the copper wire to the grounding system (Protective Earth) according to applicable regulations.
15. Using diagonal cutters or long nose pliers, remove the knockouts that cover the cable openings to the 600SS.
16. Pack both of the surge suppressor Ethernet jacks with dielectric grease.
17. Wrap a splice loop in the loose end of the Ethernet cable from the SM.
18. Connect that cable to one of the Ethernet jacks.

19. Connect an Ethernet cable to the other Ethernet jack of the 600SS and to the power adapter.
20. Replace the cover of the 600SS.
21. Connect the power supply to a power source.
22. Connect the Ethernet output from the power supply to the Ethernet port of your laptop.
23. Climb your ladder to the SM.
24. Launch your web browser.
25. In the URL address bar, enter **`169.254.1.1`**.
26. If the browser in your laptop fails to access the interface of the SM, perform the following steps:
    a. Insert your override plug into the RJ11 GPS utility port of the SM.
    NOTE: An override plug is shown in Figure 138.

Figure 138: Override plug

    b. Remove and reinsert the RJ45 Ethernet cable connector at the SM.
    NOTE: This triggers a power cycle, which causes the SM to reboot.
    c. Wait for the reboot to conclude (about 30 seconds).
    d. When the reboot is finished, remove the override plug.
    e. In the left-side menu of the SM interface, click **Login**.
    f. Consistent with local operator policy, reset both the `admin` and the `root` user passwords.
    g. In the left-side menu, click **Configuration**.
    h. Click the IP tab.
    i. Consistent with local operator practices, set an
        - **IP Address**
        - **Subnet Mask**
        - **Gateway IP Address**
    j. Click the **Save Changes** button.
    k. Click the **Reboot** button.
27. As described under Adding a User for Access to a Module on Page 430, log in as either `admin` or `root` on the SM.
28. Configure a password for the `admin` account and a password for the `root` account.
29. Log off of the SM.
30. Log back into the SM as `admin` or `root`, using the password that you configured.
31. For coarse alignment of the SM, use the Audible Alignment Tone feature as follows:
    a. In the left-side menu of the SM interface, click **Configuration**.
    b. Click the General tab.
    c. Set the **2X Rate** parameter in the SM to **Disabled**.

d. Connect the RJ-11 6-pin connector of the Alignment Tool Headset to the RJ-11 utility port of the SM.

   Alternatively, instead of using the Alignment Tool Headset, use an earpiece or small battery-powered speaker connected to Pin 5 (alignment tone output) and Pin 6 (ground) of an RJ-11 connector.

e. Listen to the alignment tone for
   - pitch, which indicates greater signal power (RSSI/dBm) by higher pitch.
   - volume, which indicates better signal quality (lower jitter) by higher volume.

Figure 139: Audible Alignment Tone kit, including headset and connecting cable

f. Adjust the module slightly until you hear the highest pitch and highest volume.

g. In the General tab of the Configuration web page of the SM, set the **2X Rate** parameter back to **Enable**.

32. When you have achieved the best signal (highest pitch, loudest volume), lock the SM in place with the mounting hardware.
33. Log off of the SM.
34. Disconnect the Ethernet cable from your laptop.
35. Replace the base cover of the SM.
36. Connect the Ethernet cable to the computer that the subscriber will be using.

Installing a PMP 400 Series SM

Installing a PMP 400 Series SM consists of two procedures:

- Physically installing the SM on a residence or other location and performing a course alignment using the alignment tone.
- Verifying the AP to SM link and finalizing alignment using review of power level, link tests, and review of registration and session counts (Procedure 24 on Page 404).

To install a PMP 400 Series (OFDM) SM, perform the following steps.

Procedure 23: Installing the OFDM SM

1. When gathering parts for the installation, select
   - a 29.5-V DC power supply and 328 feet (100 meters) or less of cable for the power supply.
   - an SMMB-2A mounting bracket
   - a 600SS surge suppressor
2. At the site, choose the best mounting location.
3. Mount the SMMB-2A bracket to thee structure.
4. Remove the base cover of the SM.
5. Terminate the UV outside grade Category 5 Ethernet cable with an RJ-45 connector, and connect the cable to the SM.
6. Wrap a drip loop in the cable.
7. Use stainless steel hose clamps or equivalent fasteners to lock the SM into position.
8. Remove the cover of the 600SS Surge Suppressor.
9. Refer to Grounding SMs on Page 178.
10. With the cable openings facing downward, mount the 600SS to the outside of the subscriber premises, as close as possible to the point where the Ethernet cable will penetrate the residence or building.
11. Using diagonal cutters or long nose pliers, remove the knockouts that cover the cable openings to the 600SS.
12. Pack both of the surge suppressor Ethernet jacks with dielectric grease.
13. Connect an Ethernet cable from the power adapter to either RJ-45 port of the 600SS.
14. Remove the bottom cover of the SM.
15. Secure a ground strap to the ground lug (circled in Figure 129 on Page 391) on the bottom of the SM.
16. Secure the ground strap to the power service panel of the structure.
17. Weather-seal the connector on the coax cable (identified by arrow in Figure 129 on Page 391).
18. Wrap a splice loop in the loose end of the Ethernet cable from the SM.
19. Connect that cable to the other RJ-45 port of the 600SS.
20. Wrap an AWG 10 (or 6mm^2) copper wire around the Ground post of the 600SS.
21. Tighten the Ground post locking nut in the 600SS onto the copper wire.
22. Securely connect the copper wire to the grounding system (Protective Earth) according to applicable regulations.
23. Replace the cover of the 600SS surge suppressor.
24. Connect the power supply to a power source.
25. Connect the Ethernet output from the power supply to the Ethernet port of your laptop.
26. Climb your ladder to the SM.
27. Launch your web browser.
28. In the URL address bar, enter **`169.254.1.1`**.
29. As described under Adding a User for Access to a Module on Page 430, log in as either `admin` or `root` on the SM.

30. Configure a password for the `admin` account and a password for the `root` account.
31. Log off of the SM.
32. Log back into the SM as `admin` or `root`, using the password that you configured.
33. For coarse alignment of the SM, use the Audible Alignment Tone feature as follows:
    a. In the left-side menu of the SM interface, click **Configuration**.
    b. Click the General tab.
    c. Set the operation rate parameter in the SM to **Disabled**.
    d. Connect the RJ-11 6-pin connector of the Alignment Tool Headset to the RJ-11 utility port of the SM.

       Alternatively, instead of using the Alignment Tool Headset, use an earpiece or small battery-powered speaker connected to Pin 5 (alignment tone output) and Pin 6 (ground) of an RJ-11 connector.
    e. Listen to the alignment tone for pitch, which indicates greater signal power (RSSI/dBm) by higher pitch.
       IMPORTANT: If you have experience in aligning FSK SMs, keep in mind that, unlike FSK SMs whose beam width is 60°, OFDM SMs have an 18 beam width. This alignment requires significantly greater precision.

       Since the OFDM SM does not measure jitter, no difference in volume is heard in the headset as you move the SM.
    f. Adjust the module slightly until you hear the highest pitch and highest volume.
    g. In the General tab of the Configuration web page of the SM, set the operation rate parameter back to the desired operation speed (1X, 2X, or 3X).
34. When you have achieved the best signal (highest pitch, loudest volume), lock the SM in place with the mounting hardware.
35. Log off of the SM.
36. Disconnect the Ethernet cable from your laptop.
37. Replace the base cover of the SM.
38. Connect the Ethernet cable to the computer that the subscriber will be using.

Configuring an AP-SM Link

To configure the AP-SM over-the-air link after the SM has been installed, perform the following steps.

Procedure 24: Configuring the AP-SM link

1. Using a computer (laptop, desktop, PDA) connected to the SM, open a browser and access the SM using the default IP address of http://169.254.1.1 (or the IP address configured in the SM, if one has been configured.)
2. In the left-side menu, select **Configuration**.
3. Click the General tab.
4. Set the **2X Rate** parameter to **Disabled**.
5. In the left-side menu, select **Tools**.
6. Click the AP Evaluation tab.

7. Among the listed APs (each shown with a unique Index number), find the AP whose **Jitter** value is lowest and whose **Power Level** value is highest (or find the ESN of the AP to which you were instructed to establish a link).
   IMPORTANT: The received **Power Level** is shown in dBm and should be maximized. **Jitter** should be minimized. However, better/lower jitter should be favored over better/higher dBm. For example, if coarse alignment gives an SM a power level of −75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to −78 dBm and the jitter to 2 or 3, the latter would be better, with the following caveats:
   - When the receiving link is operating at 1X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 4.
   - When the receiving link is operating at 2X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 9.

   An example of the AP Evaluation tab is shown in Figure 140.

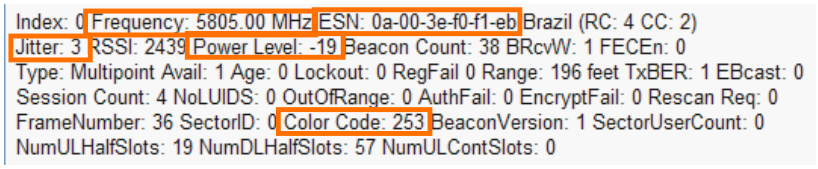

Index: 0 Frequency: 5805.00 MHz ESN: 0a-00-3e-f0-f1-eb Brazil (RC: 4 CC: 2)
Jitter: 3 RSSI: 2439 Power Level: -19 Beacon Count: 38 BRcvW: 1 FECEn: 0
Type: Multipoint Avail: 1 Age: 0 Lockout: 0 RegFail 0 Range: 196 feet TxBER: 1 EBcast: 0
Session Count: 4 NoLUIDS: 0 OutOfRange: 0 AuthFail: 0 EncryptFail: 0 Rescan Req: 0
FrameNumber: 36 SectorID: 0 Color Code: 253 BeaconVersion: 1 SectorUserCount: 0
NumULHalfSlots: 19 NumDLHalfSlots: 57 NumULContSlots: 0

Figure 140: Example data from AP Evaluation tab

   PMP 400 Series SMs do not have the **Jitter** parameter.

> ***NOTE:***
> For historical reasons, **RSSI** is also shown and is the unitless measure of power. The best practice is to use **Power Level** and ignore **RSSI**, which implies more accuracy and precision than is inherent in the measurement.

8. Write down the **Frequency** and **Color Code** values of the AP in the link.
   NOTE: See Figure 140 on Page 405.
9. In the left-side menu of the SM interface, select **Configuration**.
10. Click the Radio tab.
11. At the **Custom Radio Frequency Scan Selection List** parameter, uncheck all frequencies except the one on which the AP in the link is broadcasting.
12. At the **Color Code** parameter, enter the code number that was shown for that AP in the AP Evaluation tab.
13. Click the **Save Changes** button.
14. Click the **Reboot** button.
15. Fine-adjust the SM mounting, if needed, to improve **Jitter** (if reported) or **Power Level** according to your company standards.
    NOTE: For example, while maintaining or improving on the **Jitter** that you saw in the AP Evaluation data, and achieving ≥3 dB of **Power Level** separation from any other AP, fine-tune the SM mounting position for the highest **Power Level** achievable.
16. Retighten the hardware that secures the mounting.
17. In the left-side menu, select **Tools**.

18. Click the Link Capacity Test tab.
    NOTE: Use of this tool is described under Using the Link Capacity Test Tool (All) on Page 533.
    a. Perform several link tests of 10-second duration as follows:
    b. Type into the **Duration** field how long (in seconds) the RF link should be tested.
    c. Leave the **Packet Length** field (when present) set to the default of 1522 bytes or type into that field the packet length at which you want the test conducted.
    d. Leave the **Number of Packets** field set to 0 (to flood the link).
    e. Click the **Start Test** button.
    f. View the results of the test.
19. If these link tests fail to consistently show 90% or greater efficiency in 1X operation or 50 to 60% efficiency in 2X, troubleshoot the link, using the data as follows:
    - If the downlink is consistently 90% efficient, but the uplink is only 40%, this indicates trouble for the SM transmitting to the AP. Have link tests performed for nearby SMs. If their results are similar, investigate a possible source of interference local at the AP.
    - If the uplink is consistently 90% efficient, but the downlink is only 40%, this indicates trouble for the AP transmitting to the SM. Investigate a possible source of interference near the SM.

    If these link tests consistently show 90% or greater efficiency in 1X operation, or 50 to 60% efficiency in 2X operation, in both uplink and downlink, continue this procedure.
20. In the left-side menu, select **Configuration**.
21. In the General tab, set the **2X Rate** parameter to **Enabled**.
22. Click the **Save Changes** button.
23. If Prizm or another element management system will be used to manage the SM via SNMP, perform the following steps:
    a. Click the SNMP tab.
    b. At the **Read Permissions** parameter, select **Read/Write**.
    c. Under **Site Information**, type complete data into the three parameters: **Site Name**, **Site Contact**, **Site Location**.
    d. Click the **Save Changes** button.
24. Click the **Reboot** button.
    NOTE: At 2X operation, received **Jitter** can be as great as 9 in a high-quality downlink, but should be as low as your further aiming efforts can yield. If you need to re-aim, set the SM back to 1X operation first.

Monitoring an AP-SM Link

After the SM installer has configured the link, either an operator in the network office or the SM installer in the field (if read access to the AP is available to the installer) should perform the following procedure. Who is authorized and able to do this may depend on local operator password policy, management VLAN setup, and operational practices.

Procedure 25: Monitoring the AP-SM link for performance

1. Access the interface of the AP.
2. In the left-side menu of the AP interface, select **Home**.
3. Click the Session Status tab.
   NOTE: An example of this tab is shown in Figure 141.

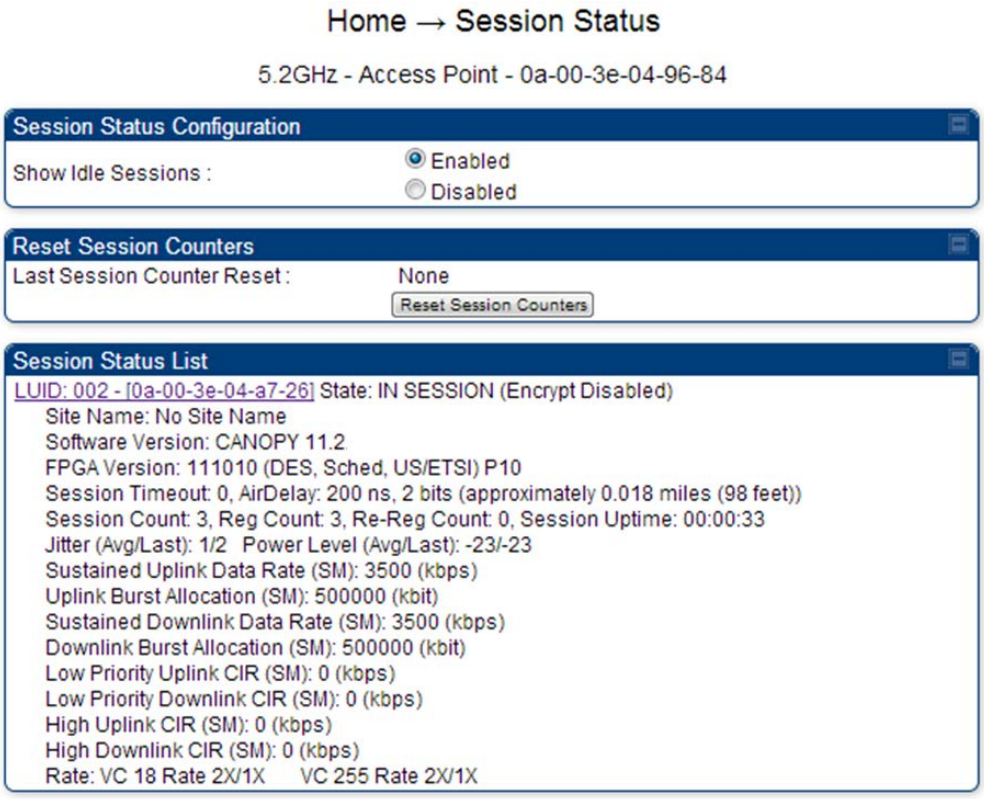

Home → Session Status
5.2GHz - Access Point - 0a-00-3e-04-96-84
Session Status Configuration
Show Idle Sessions :
Enabled
Disabled
Reset Session Counters
Last Session Counter Reset :
None
Reset Session Counters
Session Status List
LUID: 002 - [0a-00-3e-04-a7-26] State: IN SESSION (Encrypt Disabled)
Site Name: No Site Name
Software Version: CANOPY 11.2
FPGA Version: 111010 (DES, Sched, US/ETSI) P10
Session Timeout: 0, AirDelay: 200 ns, 2 bits (approximately 0.018 miles (98 feet))
Session Count: 3, Reg Count: 3, Re-Reg Count: 0, Session Uptime: 00:00:33
Jitter (Avg/Last): 1/2 Power Level (Avg/Last): -23/-23
Sustained Uplink Data Rate (SM): 3500 (kbps)
Uplink Burst Allocation (SM): 500000 (kbit)
Sustained Downlink Data Rate (SM): 3500 (kbps)
Downlink Burst Allocation (SM): 500000 (kbit)
Low Priority Uplink CIR (SM): 0 (kbps)
Low Priority Downlink CIR (SM): 0 (kbps)
High Uplink CIR (SM): 0 (kbps)
High Downlink CIR (SM): 0 (kbps)
Rate: VC 18 Rate 2X/1X VC 255 Rate 2X/1X

Figure 141: AP/SM link status indications in the AP Session Status tab

4. Find the **Session Count** line under the MAC address of the SM.
5. Check and note the values for **Session Count**, **Reg Count**, and **Re-Reg Count**.
6. Briefly monitor these values, occasionally refreshing this page by clicking another tab and then the Session Status tab again.
7. If these values are low (for example, 1, 1, and 0, respectively, meaning that the SM registered and started a stable session once) and are not changing
   a. consider the installation successful.
   b. monitor these values from the network office over the next several hours and days.

   If these values are greater than 1, 1, and 0, or they increase while you are monitoring them, troubleshoot the link. (For example, recheck jitter as described in Procedure 22: Installing the FSK SM or recheck link efficiency as described in this procedure, then look for sources of RF interference or obstructions.)

Installing a Reflector Dish

The internal patch antenna of the module illuminates the Passive Reflector Dish from an offset position. The module support tube provides the proper angle for this offset.

Both Modules Mounted at Same Elevation

For cases where the other module in the link is mounted at the same elevation, fasten the *mounting hardware leg* of the support tube vertical for each module. When the hardware leg is in this position

- the reflector dish has an obvious downward tilt.
- the *module leg* of the support tube *is not* vertical.

For a mount to a non-vertical structure such as a tapered tower, use a plumb line to ensure that the hardware leg is vertical when fastened. Proper dish, tube, and module positions for a link in this case are illustrated in Figure 142. The dish is tipped forward, not vertical, but the focus of the signal is horizontal.

Figure 142: Correct mount with reflector dish

Improper dish, tube, and module positions for this case are illustrated in Figure 143.

Figure 143: Incorrect mount with reflector dish

Modules Mounted at Different Elevations

For cases where the other module in the link is mounted at a different elevation, the assembly hardware allows tilt adjustment. The proper angle of tilt can be calculated as a factor of both the difference in elevation and the distance that the link spans. Even in this case, a plumb line and a protractor can be helpful to ensure the proper tilt. This tilt is typically minimal.

The number of degrees to offset (from vertical) the mounting hardware leg of the support tube is equal to the angle of elevation from the lower module to the higher module (b in the example provided in Figure 42 on Page 148).

Mounting Assembly

Both the hardware that Mounting Assembly 27RD provides for adjustment and the relationship between the offset angle of the module and the direction of the beam are illustrated in Figure 144.

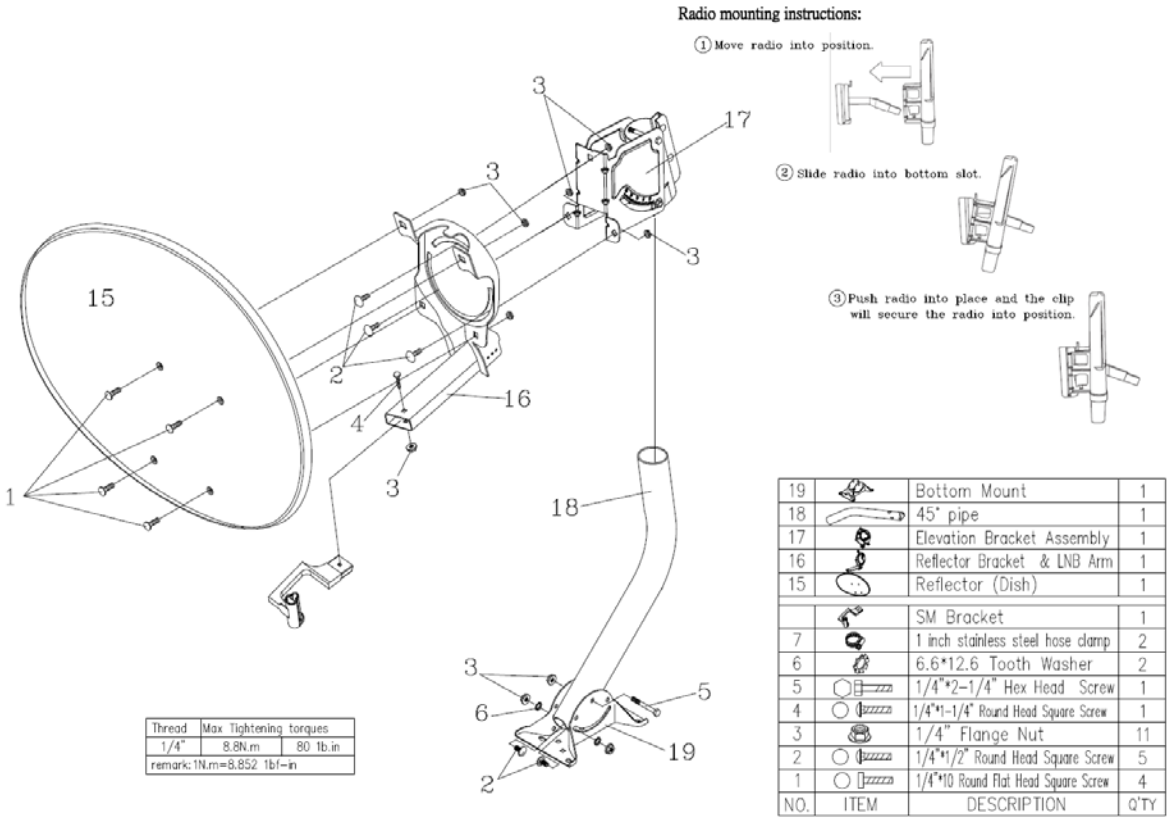

Radio mounting instructions:
① Move radio into position.
② Slide radio into bottom slot.
③ Push radio into place and the clip will secure the radio into position.
Thread | Max Tightening torques
1/4" | 8.8N.m | 80 lb.in
remark: 1N.m=8.852 lbf-in
19 Bottom Mount 1
18 45° pipe 1
17 Elevation Bracket Assembly 1
16 Reflector Bracket & LNB Arm 1
15 Reflector (Dish) 1
SM Bracket 1
7 1 inch stainless steel hose clamp 2
6 6.6*12.6 Tooth Washer 2
5 1/4"*2-1/4" Hex Head Screw 1
4 1/4"*1-1/4" Round Head Square Screw 1
3 1/4" Flange Nut 11
2 1/4"*1/2" Round Head Square Screw 5
1 1/4"*10 Round Flat Head Square Screw 4
NO. ITEM DESCRIPTION Q'TY

Figure 144: Mounting assembly, exploded view

Installing a BH Timing Master

Installing a PTP 100 Series BHM

To install a PTP 100 Series (FSK) BHM, perform the following steps.

Procedure 26: Installing the FSK BHM

1. Access the General tab of the Configuration page in the BHM.
2. If this is a 20-Mbps BH, set the **2X Rate** parameter to **Disabled** (temporarily for easier course aiming).
3. Click the **Save Changes** button.
4. Click the **Reboot** button.
5. After the reboot is completed, remove power from the BHM.
6. Choose the best mounting location for your particular application.
7. Attach the BHM to the arm of the Passive Reflector dish assembly as shown in Figure 145 or snap a LENS into place on the BHM.

RECOMMENDATION:
The arm is molded to receive and properly aim the module relative to the aim of the dish. (See Figure 142 on Page 408.) Stainless steel hose clamps should be used for the attachment.

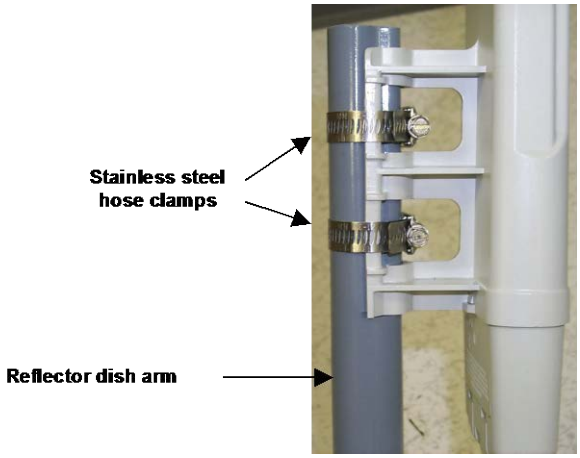


Figure 145: BH attachment to reflector arm

8. Align the BHM as follows:
   a. Move the module to where the link will be unobstructed by the radio horizon and no objects penetrate the Fresnel zone. (The Canopy System Calculator page AntennaElevationCalcPage.xls automatically calculates the minimum antenna elevation that is required to extend the radio horizon to the other end of the link. The Canopy System Calculator page FresnelZoneCalcPage.xls automatically calculates the Fresnel zone clearance that is required between the visual line of sight and the top of a high-elevation object.)
   b. Use a local map, compass, and/or GPS device as needed to determine the direction to the BHS.
   c. Apply the appropriate degree of downward or upward tilt. (The Canopy System Calculator page DowntiltCalcPage.xls automatically calculates the angle of antenna downward tilt that is required.)
   d. Ensure that the BHS is within the beam coverage area. (The Canopy System Calculator page BeamwidthRadiiCalcPage.xls automatically calculates the radii of the beam coverage area.)
9. Using stainless steel hose clamps or equivalent fasteners, lock the BHM into position.
10. Remove the base cover of the BHM. (See Figure 55 on Page 184.)
11. If this BHM *will not* be connected to a CMM, optionally connect a utility cable to a GPS timing source and then to the RJ-11 port of the BHM.
12. Either connect the BHM to the CMM or connect the DC power converter to the BHM and then to an AC power source.
    RESULT: When power is applied to a module or the unit is reset on the web-based interface, the module requires approximately 25 seconds to boot. During this interval, self-tests and other diagnostics are being performed.

13. Access the General tab of the Configuration page of this BHM.
14. If a CMMmicro or CMM4 is connected, set the **Sync Input** parameter to the **Sync to Received Signal (Power Port)** selection.

    If a CMM2 is connected, set the **Sync Input** parameter to the **Sync to Received Signal (Timing Port)** selection.

Installing a PTP 200 Series BHM

To install a PTP 200 Series (OFDM) BHM, use the procedure provided under Installing a PMP 400 Series AP on Page 386, with the following additional treatment for a setting that is unique to PTP 200 Series wireless Ethernet bridges.

OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol (slot) to allow multipathing to settle before receiving the desired data. A 1/4 cyclic prefix means that for every 4 bits of throughput data transmitted, an additional bit is used, A 1/8 cyclic prefix means that for every 8 bits of throughput data transmitted, an additional bit is used.

PTP 200 Series modules (OFDM BHs) are settable for either 1/8 or 1/4 cyclic prefix. The use of 1/8 cyclic prefix provides about 11% higher maximum throughput and is recommended for most cases.

The **Cyclic Prefix** is set on the Configuration => Radio page of the BHM. The default on a new unit or after the unit has been reset to factory defaults is 1/4 Cyclic Prefix. In most deployments, 1/8 Cyclic Prefix will provide a high quality, higher throughput link. In cases with severe multipathing or obstructions, 1/4 Cyclic Prefix may yield better overall results.

Procedure 27: Setting the Cyclic Prefix in a PTP 200 Series wireless Ethernet bridge

1. Before deployment, set the **Cyclic Prefix** on the Configuration => Radio page of both the BHM and the BHS to 1/8.
   IMPORTANT: The **Cyclic Prefix** setting must be identical in both the BHM and the BHS. If the settings do not match, then the BHS will not register in the BHM.
2. During installation, use Link Tests to confirm link quality per standard installation and alignment procedures.
3. If a Link Test shows low throughput or efficiency, consider changing the **Cyclic Prefix** setting to 1/4 on both the BHM and the BHS along with other standard installation troubleshooting procedures such as re-aiming, off-axis aiming, changing location, raising or lowering the height of the radio, and adjusting the **Transmitter Output Power** setting.

Installing a BH Timing Slave

Installing a PTP 100 Series BHS

Installing a PTP 100 Series (FSK) BHS consists of two procedures:

- Physically installing the BHS and performing a course alignment using the alignment tone (Procedure 28).
- Verifying the BH link and finalizing alignment using review of power level and jitter, link tests, and review of registration and session counts (Procedure 29 on Page 415).

Procedure 28: Installing the FSK BHS

1. Choose the best mounting location for the BHS.
2. Remove the base cover of the BHS. (See Figure 55 on Page 184.)
3. Terminate the UV outside grade Category 5 Ethernet cable with an RJ-45 connector, and connect the cable to the BHS. (See Procedure 8 on Page 199.)
4. Attach the BHS to the arm of the Passive Reflector dish assembly as shown in Figure 135 on Page 398 or snap a LENS onto the BHS.

RECOMMENDATION:
The arm is molded to receive and properly aim the BH relative to the aim of the dish. Use stainless steel hose clamps for the attachment.

5. Use stainless steel hose clamps or equivalent fasteners to lock the BHS into position.
6. Remove the cover of the 600SS Surge Suppressor.
7. With the cable openings facing downward, mount the 600SS as close to the grounding system (Protective Earth) as possible.
8. Using diagonal cutters or long nose pliers, remove the knockouts that cover the cable openings to the 600SS.
9. Connect an Ethernet cable from the power adapter to either RJ-45 port of the 600SS.
10. Connect another Ethernet cable from the other RJ-45 port of the 600SS to the Ethernet port of the BHS.
11. Refer to Grounding SMs on Page 178.
12. Wrap an AWG 10 (or 6mm^2) copper wire around the Ground post of the 600SS.
13. Tighten the Ground post locking nut in the 600SS onto the copper wire.
14. Securely connect the copper wire to the grounding system (Protective Earth) according to applicable regulations.
15. Connect a ground wire to the 600SS.
16. Replace the cover of the 600SS surge suppressor.
17. For coarse alignment of the BHS, use the Audible Alignment Tone feature as follows:
18. If the Configuration web page of the BHS contains a **2X Rate** parameter, set it to **Disable**.
    a. At the BHS, connect the RJ-11 6-pin connector of the Alignment Tool Headset (shown in Figure 139 on Page 402) to the RJ-11 utility port of the SM.

       Alternatively, instead of using the Alignment Tool Headset, use an earpiece or small battery-powered speaker connected to Pin 5 (alignment tone output) and Pin 6 (ground) of an RJ-11 connector.

b. Listen to the alignment tone for
   - pitch, which indicates greater signal power (RSSI/dBm) by higher pitch.
   - volume, which indicates better signal quality (lower jitter) by higher volume.

c. Adjust the module slightly until you hear the highest pitch and highest volume.

d. If the Configuration web page of the BHS contains a **2X Rate** parameter, set it back to **Enable**.

19. When you have achieved the best signal (highest pitch, loudest volume), lock the BHS in place with the mounting hardware.

Installing a PTP 200 Series BHS

To install a PTP 200 Series (OFDM) BHM, use the procedure provided under Installing a PMP 400 Series SM on Page 402, with the following additional treatment for a setting that is unique to PTP 200 Series wireless Ethernet bridges.

OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol (slot) to allow multipathing to settle before receiving the desired data. A 1/4 cyclic prefix means that for every 4 bits of throughput data transmitted, an additional bit is used, A 1/8 cyclic prefix means that for every 8 bits of throughput data transmitted, an additional bit is used.

PTP 200 Series modules (OFDM BHs) are settable for either 1/8 or 1/4 cyclic prefix. The use of 1/8 cyclic prefix provides about 11% higher maximum throughput and is recommended for most cases.

The **Cyclic Prefix** is set on the Configuration => Radio page of the BHM. The default on a new unit or after the unit has been reset to factory defaults is 1/4 Cyclic Prefix. In most deployments, 1/8 Cyclic Prefix will provide a high quality, higher throughput link. In cases with severe multipathing or obstructions, 1/4 Cyclic Prefix may yield better overall results.

To perform and possibly adjust the setting, use Procedure 27: Setting the Cyclic Prefix in a PTP 200 Series wireless Ethernet bridge on Page 412.

Upgrading a BH Link to BH20

To replace a pair of 10-Mbps BHs with 20-Mbps BHs, you can minimize downtime by temporarily using the 10-Mbps capability in the faster modules. However, both interference and differences in receiver sensitivity can make alignment and link maintenance more difficult than in the previous 10-Mbps link. The effects of these factors are greater at greater link distances, particularly at 5 miles or more.

In shorter spans, these factors may not be prohibitive. For these cases, set the first replacement module to **1X Rate** and establish the link to the 10-Mbps BH on the far end. Similarly, set the second replacement module to **1X Rate** and re-establish the link. With both of the faster modules in place and with an operational link having been achieved, reset their modulation to **2X Rate** (20 Mbps).

Verifying a BH Link

To verify the backhaul link after the BHS has been installed, perform the following steps.

Procedure 29: Verifying performance for a BH link

1. Using a computer (laptop, desktop, PDA) connected to the BHS, open a browser and access the BHS using the default IP address of http://169.254.1.1 (or the IP address configured in the BHS, if one has been configured.)
2. On the General Status tab of the Home page in the BHS (shown in Figure 73 on Page 224), look for **Power Level** and **Jitter**.
   IMPORTANT: The received **Power Level** is shown in dBm and should be maximized. **Jitter** should be minimized. However, better/lower jitter should be favored over better/higher dBm. For example, if coarse alignment gives a BHS a power level of −75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to −78 dBm and the jitter to 2 or 3, the latter would be better, with the following caveats:
   - When the receiving link is operating at 1X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 4.
   - When the receiving link is operating at 2X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 9.

PTP 200 Series BHSs do not have this parameter.

NOTE:
For historical reasons, **RSSI** is also shown and is the unitless measure of power. The best practice is to use **Power Level** and ignore **RSSI**, which implies more accuracy and precision than is inherent in its measurement.

3. Fine-adjust the BHS mounting, if needed, to improve **Jitter** or **Power Level**.
4. Click the Link Capacity Test tab of the Tools web page in the BHS.
   NOTE: Use of this tool is described under Using the Link Capacity Test Tool (All) on Page 533.
5. Perform several link tests of 10-second duration as follows:
   a. Type into the **Duration** field how long (in seconds) the RF link should be tested.
   b. Leave the **Packet Length** field (when present) set to the default of 1522 bytes or type into that field the packet length at which you want the test conducted.
   c. Leave the **Number of Packets** field set to 0 (to flood the link).
   d. Click the **Start Test** button.
   e. View the results of the test.

6. If these link tests fail to consistently show 90% or greater efficiency in 1X operation or 50 to 60% efficiency in 2X, troubleshoot the link, using the data as follows:
   - If the downlink is consistently 90% efficient, but the uplink is only 40%, this indicates trouble for the BHS transmitting to the BHM. Investigate a possible source of interference near the BHM.
   - If the uplink is consistently 90% efficient, but the downlink is only 40%, this indicates trouble for the BHM transmitting to the BHS. Investigate a possible source of interference near the BHS.

   If these link tests consistently show 90% or greater efficiency in 1X operation, or 50 to 60% efficiency in 2X operation, in both uplink and downlink, continue this procedure.
7. Open the Session Status tab in the Home page of the BHM.
8. Find the **Session Count** line under the MAC address of the BHS.
9. Check and note the values for **Session Count**, **Reg Count**, and **Re-Reg Count**.
10. Briefly monitor these values, occasionally refreshing this page by clicking another tab and then the Session Status tab again.
11. If these values are low (for example, 1, 1, and 0, respectively, meaning that the BHS registered and started a stable session once) and not changing
    a. consider the installation successful.
    b. monitor these values from the network office over the next several hours and days.

    If these values are greater than 1, 1, and 0, or they increase while you are monitoring them, troubleshoot the link. (For example, recheck jitter as described in Procedure 22: Installing the FSK SM or recheck link efficiency as described in this procedure, then look for sources of RF interference or obstructions.)

Chapter 20: Verifying System Functionality

To verify system functionality after the APs and or BHs have been installed, perform the following steps.

Procedure 30: Verifying system functionality

1. For each installed AP, use a computer or PDA connected to an SM set to a compatible configuration (frequency and color code, for example) and verify link functionality.
2. For each BH installed, use a notebook computer connected to a BH (BHM or BHS, as appropriate) set to a compatible configuration and verify link functionality.
3. If a network data feed is present and operational, use an SM or BHS to verify network functionality.

Operations Guide

Chapter 21: Growing Your Network

Keys to successfully growing your network include

- monitoring the RF environment.
- considering software release compatibility.
- redeploying modules appropriately and quickly.

Monitoring the RF Environment

Regardless of whether you are maintaining or growing your network, you may encounter new RF traffic that can interfere with your current or planned equipment. Regularly measuring *over a period of time* and logging the RF environment, as you did before you installed your first equipment in an area, enables you to recognize and react to changes.

Spectrum Analyzer

In both an FSK and an OFDM module, the spectrum analyzer measures and displays the detected *peak* power level. This is consistent with the received Power Level that various tabs in the FSK modules report. However, it is inconsistent with received Power Level indications in OFDM modules, which use this parameter to report the detected *average* power level. For this reason, you will observe a difference in how the spectrum analyzer and the Power Level field separately report on the same OFDM signal at the same time.

The integrated spectrum analyzer can be very useful as a tool for troubleshooting and RF planning, but is not intended to replicate the accuracy and programmability of a high-end spectrum analyzer, which you may sometime need for other purposes.

IMPORTANT!

When you enable the Spectrum Analyzer on a module, it enters a scan mode and drops any RF connection it may have had. Scanning mode ends when either you click **Disable** on the Spectrum Analyzer page, or it times out after 15 minutes and returns to operational mode.

For this reason

- *do not* enable the spectrum analyzer on a module you are connected to via RF. The connection will drop for 15 minutes, and when the connection is re-established no readings will be displayed.
- be advised that, if you enable the spectrum analyzer by Ethernet connection, the RF connection to that module drops.

You can use any module to see the frequency and power level of any detectable signal that is within, just above, or just below the frequency band range of the module.

RECOMMENDATION:
Vary the days and times when you analyze the spectrum in an area.
The RF environment can change throughout the day or throughout the week.

Temporarily deploy an SM or BHS for *each* frequency band range that you need to monitor and access the Spectrum Analyzer tab in the Tools web page of the module. (For access from a PDA, see PDA Access to Modules on Page 385.) To enter the scan mode and view readings, click **Enable**.

After clicking the **Enable** button on the Spectrum Analyzer page, the first "painting" may not display bars for all frequencies, especially on frequency bands with a large number of center channels, like the 5.4 GHz band. Clicking **Enable** again will display the entire spectrum bar graph. Alternatively, you can set the "Auto Refresh" time on the Configuration => General page to a few seconds to have the Spectrum Analyzer automatically fully displayed and refreshed. (Setting the "Auto Refresh" time back to 0 will disable refresh.)

Graphical Spectrum Analyzer Display

An SM/BHS displays the graphical spectrum analyzer. An example of the Spectrum Analyzer tab is shown in Figure 146.

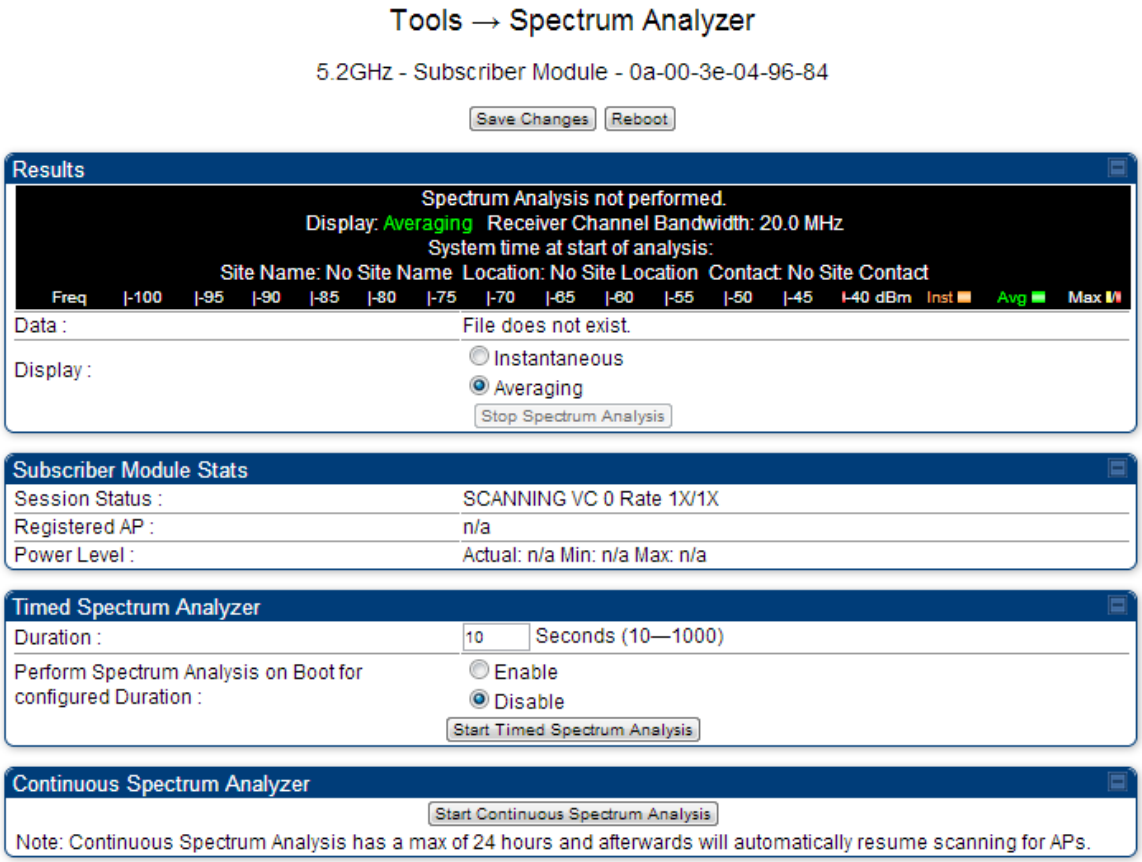

Tools → Spectrum Analyzer
5.2GHz - Subscriber Module - 0a-00-3e-04-96-84
Save Changes
Reboot
Results
Spectrum Analysis not performed.
Display: Averaging Receiver Channel Bandwidth: 20.0 MHz
System time at start of analysis:
Site Name: No Site Name Location: No Site Location Contact: No Site Contact
Freq -100 -95 -90 -85 -80 -75 -70 -65 -60 -55 -50 -45 -40 dBm Inst Avg Max
Data : File does not exist.
Display : Instantaneous
Averaging
Stop Spectrum Analysis
Subscriber Module Stats
Session Status : SCANNING VC 0 Rate 1X/1X
Registered AP : n/a
Power Level : Actual: n/a Min: n/a Max: n/a
Timed Spectrum Analyzer
Duration : 10 Seconds (10—1000)
Perform Spectrum Analysis on Boot for configured Duration : Enable
Disable
Start Timed Spectrum Analysis
Continuous Spectrum Analyzer
Start Continuous Spectrum Analysis
Note: Continuous Spectrum Analysis has a max of 24 hours and afterwards will automatically resume scanning for APs.

Figure 146: Spectrum Analyzer tab of SM, example

Colors in the display have the following meanings:

- Green bars show the most recent measurements.
- Yellow ticks show the maximum measurements from the current spectrum analysis session.
- Red ticks show measurements of −40 dBm or stronger.

To keep the displayed data current, either set “Auto Refresh” on the module’s Configuration => General page to a few seconds, or repeatedly click the **Enable** button. When you are finished analyzing the spectrum, click the **Disable** button to return the module to normal operation.

Using the AP as a Spectrum Analyzer

You can temporarily change an AP into an SM and thereby use the spectrum analyzer functionality. This is the only purpose supported for the transformation.

CAUTION!

When you change an AP into an SM, any connections to SMs off that AP are lost. Therefore, you should ensure you are connected to the AP through its *Ethernet* side (not RF side) before changing it into an SM.

For example, if you are connected to an AP through one of its SMs and mistakenly change the AP into an SM, you will lose connectivity and will need to gain access to the Ethernet side of the AP through another part of your network to change it back into an AP.

To transform a VLAN-disabled AP into an SM for spectrum analysis and then return the device to an AP, perform the following steps.

Procedure 31: Using the Spectrum Analyzer in AP feature, VLAN disabled

1. Connect to the wired Ethernet interface of the AP.
2. Access the General tab of the Configuration page in the AP.
3. Set the **Device Setting** parameter to **SM**.
4. Click the **Save Changes** button.
5. Click the **Reboot** button.
6. When the module has rebooted as an SM, click the Tools navigation link on the left side of the Home page.
7. Click the Spectrum Analyzer tab.
   NOTE: If you simply click the **Enable** button on the Spectrum Analyzer tab, the display may include fewer than all frequencies that are detectable, especially in a band, such as 5.4 GHz, where the number of available center channels is great. If you then click the **Enable** button a second time or set the **Webpage Auto Update** parameter in the Configuration => General tab to a few seconds, the display includes the entire spectrum. You can later reset **Webpage Auto Update** to **0**, to disable refresh.
8. Either set the **Webpage Auto Update** parameter in the Configuration => General tab to a few seconds or repeatedly click the **Enable** button.
   RESULT: The module enters the scan mode.
9. When you are finished analyzing the spectrum, click the **Disable** button.
10. In the left-side navigation links, click Configuration.
11. Click the General tab.
12. Set the **Device Setting** parameter to **AP**.
13. Click the **Save Changes** button.
14. Click the **Reboot** button.
    RESULT: The AP boots with its previous frequency setting.

If you reboot an AP that has a configured **Management VID** parameter and **Device Type** parameter set to **SM**, you are automatically removing the AP from the Management VLAN. The following procedure enables you to successfully analyze the spectrum and return to management via the VLAN feature. In many cases, it is advisable to use this procedure to

1. transform all APs in a cluster into SMs.
2. perform spectrum analysis without Management VLAN, one sector at a time.
3. return all APs in the cluster to their Management VLAN for access.

To transform a VLAN-enabled AP into an SM for spectrum analysis and then return the device to an AP, perform the following steps.

Procedure 32: Using the Spectrum Analyzer in AP feature, VLAN enabled

1. Access the VLAN-enabled AP through its Management VLAN.
   NOTE: How you do this depends on your local configuration.
2. Access the General tab of the Configuration page in the AP.
3. Set the **Device Setting** parameter to **SM**.
4. Click the **Save Changes** button.
5. Click the **Reboot** button.
   RESULT: Connectivity to the module is lost.
6. Access the module without using the Management VLAN.
   NOTE: How you do this depends on your local configuration. You may need to connect to a different, non-tagging port of the VLAN switch in your NOC.
7. Click the Tools navigation link on the left side of the Home page.
8. Click the Spectrum Analyzer tab.
   NOTE: If you simply click the **Enable** button on the Spectrum Analyzer tab, the display may include fewer than all frequencies that are detectable, especially in a band, such as 5.4 GHz, where the number of available center channels is great. If you then click the **Enable** button a second time or set the **Webpage Auto Update** parameter in the Configuration => General tab to a few seconds, then the display will include the entire spectrum.
9. Either set the **Webpage Auto Update** parameter in the Configuration => General tab to a few seconds or repeatedly click the **Enable** button.
   RESULT: The module enters the scan mode.
10. When you are finished analyzing the spectrum, click the **Disable** button.
11. In the left-side navigation links, click Configuration.
12. Click the General tab.
13. Set the **Device Setting** parameter to AP.
14. Click the **Save Changes** button.
15. Click the **Reboot** button.
    RESULT: Connectivity to the module is lost.
16. Access the AP through its Management VLAN.
    NOTE: How you do this depends on your local configuration. You may need to connect to the appropriate tagging port of the VLAN switch in your NOC.

Considering Software Release Compatibility

Within the same network, modules can operate on multiple software releases. However, the features that can be enabled are limited to those that the earliest software supports.

Designations for Hardware in Radios

Documentation refers to hardware series (for example, Series P9). Releases 8 and later requires APs, BHs, and AES SMs to be Series P9 or later hardware. The correlation between hardware series and the MAC addresses of the radio modules is provided in Table 61.

Table 61: Hardware series by MAC address

Radio Frequency Band Range	Hardware Series	
	P7 or P8 in These MAC Addresses	P9 or Later in These MAC Addresses
900	None	All
2.4	≤ 0A003E20672B	≥ 0A003E20672C
5.2	≤ 0A003E00F4E3	≥ 0A003E00F4E4
5.4	None	All
5.7	≤ 0A003EF12AFE	≥ 0A003EF12AFF

Differences in capabilities among these hardware series are summarized in Table 62.

Table 62: Hardware series differences

Capability	Availability per Hardware Series		
	P7	P8	P9, P10, or P11
Auto-sense Ethernet cable scheme	no	yes	yes
Support CMMmicro	no	yes	yes
Support CMM4	no	yes	yes
Support hardware scheduling in APs	no	no	yes
Support 2X operation in APs and SMs	no	no	yes
NOTES: An SM of P7 or P8 series requires an FPGA load through CNUT for access to hardware scheduling, and then only at 1X operation. An AP of P7 or P8 series cannot perform hardware scheduling.			

CAP 130 P9 APs provide higher throughput and lower latency than earlier series APs and support configuring the high-priority channel per SM. CAP 120 APs *do not* provide the higher throughput and lower latency, but they do support configuring the high-priority channel per SM.

MIB File Set Compatibility

Although MIB files are text files (not software), they define objects associated with configurable parameters and indicators for the module and its links. In each release, some of these parameters and indicators are not carried forward from the previous release, and some parameters and indicators are introduced or changed.

For this reason, use the MIB files from your download to replace previous MIB files in conjunction with your software upgrades, even if the file names are identical to those of your previous files. Date stamps on the MIB files distinguish the later set.

Redeploying Modules

Successfully redeploying a module may involve

- maintaining full and accurate records of modules being redeployed from warehouse stock.
- exercising caution about
  - software compatibility. For example, whether desired features can be enabled with the redeployed module in the network.
  - procedural handling of the module. For example
    - whether to align the SM or BHS by power level and jitter or by only jitter.
    - whether the module auto-senses the Ethernet cable connector scheme.
  - hardware compatibility; for example, where a CMMmicro is deployed.
  - the value of each configurable parameter. Whether all are compatible in the new destination.
- remembering to use auto discovery to add the redeployed SM to the network in Prizm.

Wiring to Extend Network Sync

The following procedure can be used to extend network sync by one additional hop, as described under Passing Sync in an Additional Hop on Page 96. Where a co-located module receives sync over the air, the co-located modules can be wired to pass the sync as follows:

Procedure 33: Extending network sync

1. Connect the GPS Utility ports of the co-located modules using a sync cable with RJ-11 connectors.
2. Set the **Sync Input** parameter on the Configuration page of the co-located AP or BH timing master to **Sync to Received Signal (Timing Port)**.

3. Set the **Frame Timing Pulse Gated** parameter on the Configuration page of the co-located SM or BH timing slave to **Enable**.
   NOTE: This setting prevents interference in the event that the SM or BH timing slave loses sync.

Chapter 22: Securing Your Network

Isolating APs from the Internet

Ensure that the IP addresses of the APs in your network

- are not routable over the Internet.
- do not share the subnet of the IP address of your user.

RFC 1918, *Address Allocation for Private Subnets*, reserves for private IP networks three blocks of IP addresses that are not routable over the Internet:

- /8 subnets have one reserved network, 10.0.0.0 to 10.255.255.255.
- /16 subnets have 16 reserved networks, 172.16.0.0 to 172.31.255.255.
- /24 subnets have 256 reserved networks, 192.168.0.0 to 192.168.255.255.

Encrypting Radio Transmissions

Cambium fixed wireless broadband IP systems employ the following forms of encryption for security of the wireless link:

- DES–Data Encryption Standard, an over-the-air link option that uses secret 56-bit keys and 8 parity bits.
- AES–Advanced Encryption Standard, an extra-cost over-the-air link option that provides extremely secure wireless connections. AES uses 128-bit secret keys as directed by the government of the U.S.A. AES is not exportable and requires a special AP to process the large keys.

DES Encryption

Standard modules provide DES encryption. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES Encryption does not affect the performance or throughput of the system.

AES Encryption

Cambium also offers fixed wireless broadband IP network products that provide AES encryption. AES uses the Rijndael algorithm and 128-bit keys to establish a higher level of security than DES. Because of this higher level of security, the government of the U.S.A. controls the export of communications products that use AES (among which the AES feature activation key is one) to ensure that these products are available in only certain regions and by special permit.

The distributor or reseller can advise service providers about current regional availability. AES products are certified as compliant with the Federal Information Processing Standards (FIPS) in the U.S.A. The National Institute of Standards and Technology (NIST) in the U.S.A. has specified AES for significantly greater security than that which DES provides. NIST selected the AES algorithm for providing the best combination of security, performance, efficiency, implementation, and flexibility. NIST collaborates with industry to develop and apply technology, measurements, and standards.

AES-DES Operability Comparisons

This section describes the similarities and differences between DES and AES products, and the extent to which they may interoperate.

The DES AP and the DES BHM modules are factory-programmed to enable or disable *DES* encryption. Similarly, the AES AP and the AES BHM modules are factory-programmed to enable or disable *AES* encryption. In either case, the authentication key entered in the Configuration page establishes the encryption key. For this reason, the authentication key must be the same on each end of the link.

Feature Availability

AES products run the same software as DES products. Thus feature availability and functionality are and will continue to be the same, regardless of whether AES encryption is enabled. All interface screens are identical. However, when encryption is enabled on the Configuration screen

- the AES product provides AES encryption.
- the DES product provides DES encryption.

AES and DES products use different FPGA (field-programmable gate array) loads. However, the AES FPGA will be upgraded as needed to provide new features or services similar to those available for DES products.

Canopy DES products cannot be upgraded to AES. To have the option of AES encryption, the operator must purchase AES products.

Interoperability

AES and DES products do not interoperate when enabled for encryption. For example, An AES AP with encryption enabled cannot communicate with DES SMs. Similarly, an AES Backhaul timing master module with encryption enabled cannot communicate with a DES Backhaul timing slave module.

However, if encryption is disabled, AES modules can communicate with DES modules.

Managing Module Access by Passwords

Adding a User for Access to a Module

From the factory, each module has a preconfigured administrator-level account in the name `root`, which initially requires no associated password. This is the same `root` account that you may have used for access to the module by `telnet` or `ftp`. When you upgrade a module

- an account is created in the name `admin`.
- both `admin` and `root` inherit the password that was previously used for access to the module:
  - the **Full Access** password, if one was set.
  - the **Display-Only Access** password, if one was set and no Full Access password was set.

IMPORTANT!

If you use Prizm, *do not* delete the `root` account from any module. If you use an NMS that communicates with modules through SNMP, *do not* delete the `root` account from any module unless you first can confirm that the NMS does not rely on the `root` account for access to the modules.

Each module supports four or fewer user accounts, regardless of account levels. The available levels are

- ADMINISTRATOR, who has full read and write permissions. This is the level of the `root` and `admin` users, as well as any other administrator accounts that one of them creates.
- INSTALLER, who has permissions identical to those of ADMINISTRATOR except that the installer cannot add or delete users or change the password of any other user.
- GUEST, who has no write permissions and only a limited view of General Status tab, as shown in Figure 147, and can log in as a user.

From the factory default state, configure passwords for both the `root` and `admin` account at the ADMINISTRATOR permission level, using the Account => Change Users Password tab. (If you configure only one of these, then the other will still require no password for access into it and thus remain a security risk.) If you are intent on configuring only one of them, delete the `admin` account. The `root` account is the only account that CNUT uses to update and Prizm uses to manage the module.

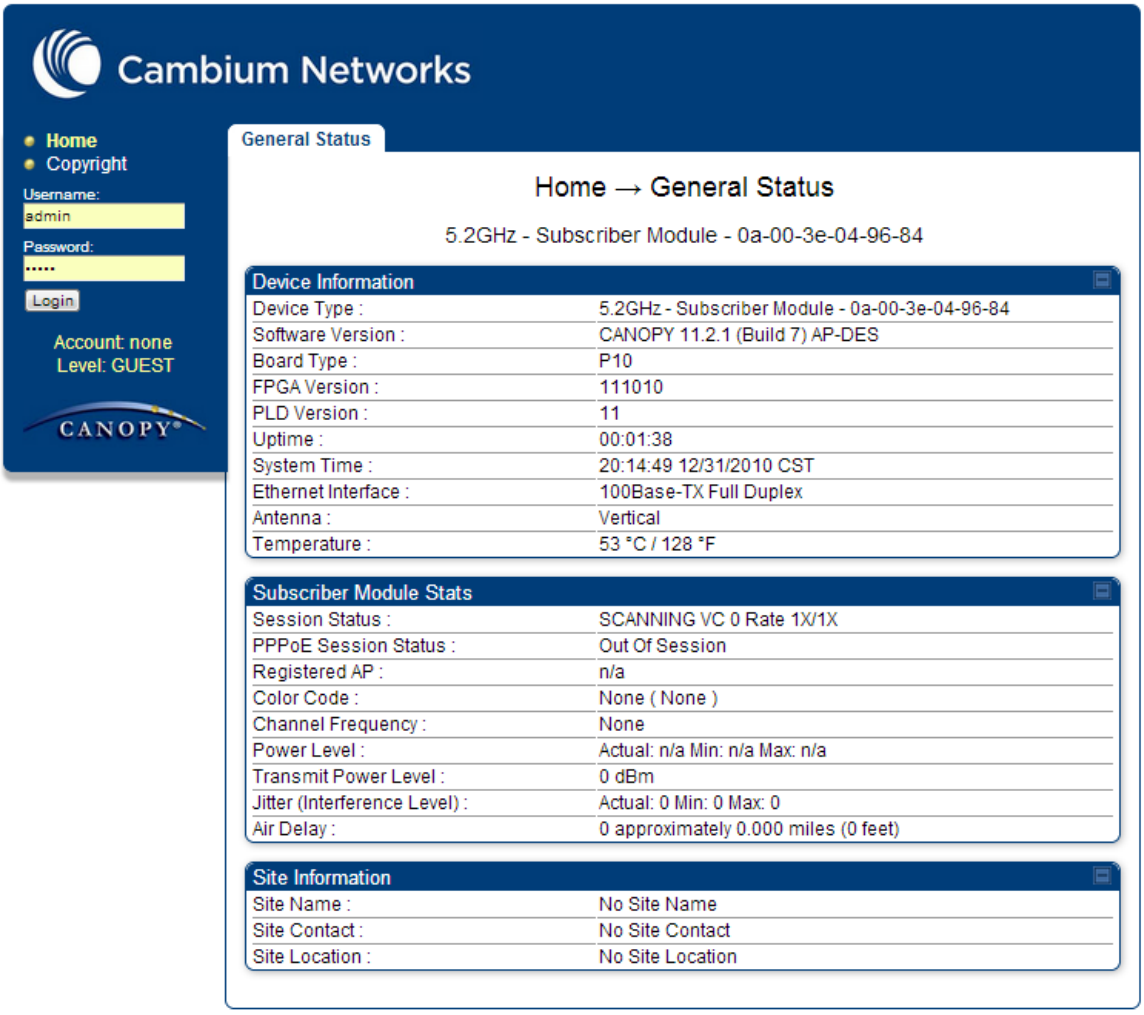

Cambium Networks
Home
Copyright
Username:
admin
Password:
Login
Account: none
Level: GUEST
CANOPY
General Status
Home → General Status
5.2GHz - Subscriber Module - 0a-00-3e-04-96-84
Device Information
Device Type : 5.2GHz - Subscriber Module - 0a-00-3e-04-96-84
Software Version : CANOPY 11.2.1 (Build 7) AP-DES
Board Type : P10
FPGA Version : 111010
PLD Version : 11
Uptime : 00:01:38
System Time : 20:14:49 12/31/2010 CST
Ethernet Interface : 100Base-TX Full Duplex
Antenna : Vertical
Temperature : 53 °C / 128 °F
Subscriber Module Stats
Session Status : SCANNING VC 0 Rate 1X/1X
PPPoE Session Status : Out Of Session
Registered AP : n/a
Color Code : None (None)
Channel Frequency : None
Power Level : Actual: n/a Min: n/a Max: n/a
Transmit Power Level : 0 dBm
Jitter (Interference Level) : Actual: 0 Min: 0 Max: 0
Air Delay : 0 approximately 0.000 miles (0 feet)
Site Information
Site Name : No Site Name
Site Contact : No Site Contact
Site Location : No Site Location

Figure 147: General Status tab view for GUEST-level account

An example of the Add User tab is displayed in Figure 148.

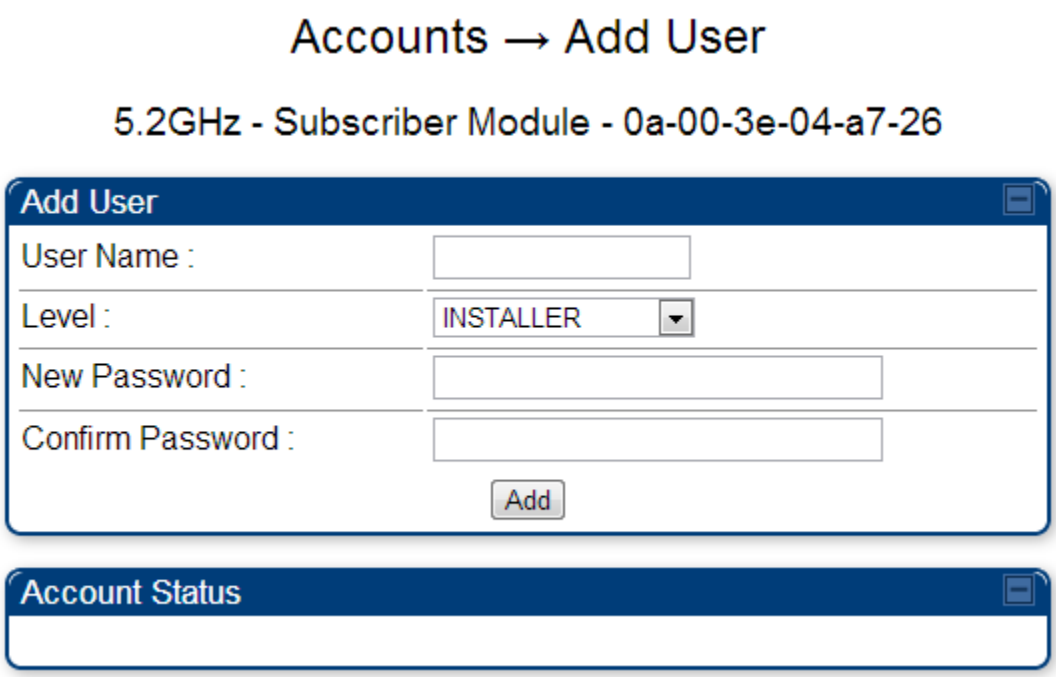


Figure 148: Add User tab of SM, example

After a password has been set for any ADMINISTRATOR-level account, initial access to the module GUI opens the view of GUEST level (Figure 147).

Deleting a User from Access to a Module

The Account => Delete User tab provides a drop-down list of configured users from which to select the user you want to delete.

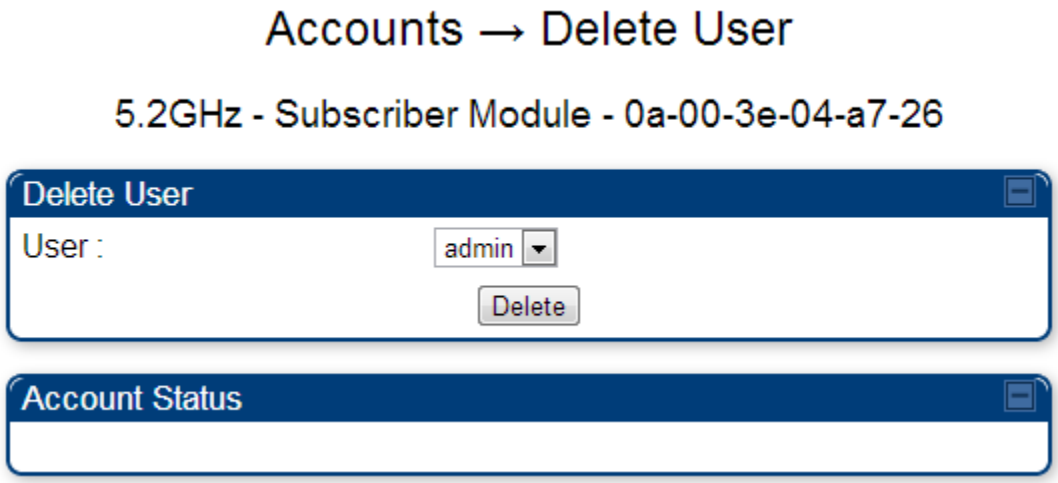


Figure 149: Delete User tab of SM, example

Accounts that cannot be deleted are

- the current user's own account.
- the last remaining account of ADMINISTRATOR level.

Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH

A small adjunctive product allows you to temporarily override some AP/SM/BH settings and thereby regain control of the module. This override plug is needed for access to the module in any of the following cases:

- You have forgotten either
  - the IP address assigned to the module.
  - the password that provides access to the module.
- You want local access to a module that has had the 802.3 link disabled in the Configuration page.

You can configure the module such that, when it senses the override plug, it responds by either

- resetting the LAN1 IP address to 169.254.1.1, allowing access through the default configuration without *changing* the configuration, whereupon you will be able to view and reset any non-default values as you wish.
- resetting all configurable parameters to their factory default values.

Acquiring the Override Plug

You can either purchase or fabricate an override plug as follows. To purchase an override plug for a nominal fee, order the plug at http://www.best-tronics.com/cambium.htm . To fabricate an override plug, perform the following steps.

Procedure 34: Fabricating an override plug

1. Install an RJ-11 6-pin connector onto a 6-inch length of CAT 5 cable.
2. Pin out all 6-pins.
3. Short (solder together) Pins 4 and 6 on the other end. Do not connect any other wires to anything. The result should be as shown in
4. Figure 150.

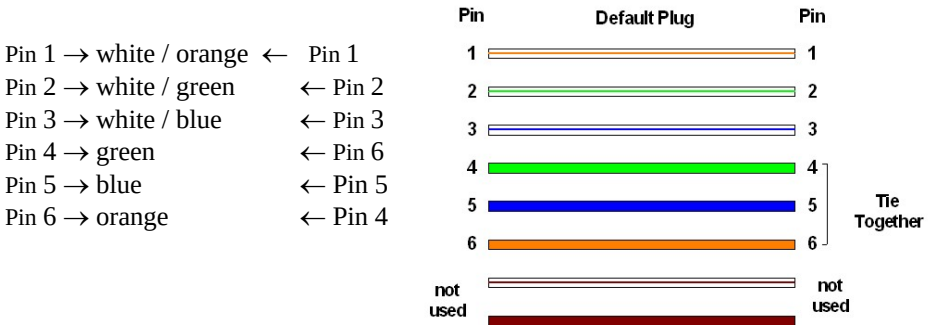


Figure 150: RJ-11 pinout for the override plug

Using the Override Plug

IMPORTANT!
While the override plug is connected to a module, the module can neither register nor allow registration of another module.

To regain access to the module, perform the following steps.

Procedure 35: Regaining access to a module

1. Insert the override plug into the RJ-11 GPS utility port of the module.
2. Power cycle by removing, then re-inserting, the Ethernet cable.
   RESULT: The module boots with the default IP address of 169.254.1.1, password fields blank, and all other configuration values as previously set.
3. Wait approximately 30 seconds for the boot to complete.
4. Remove the override plug.
5. Set passwords and IP address as desired.
6. Change configuration values if desired.
7. Click the **Save Changes** button.
8. Click the **Reboot** button.

Requiring SM Authentication

By using a RADIUS server in the management network, SMs may be required to authenticate before being allowed entry into the network. SM authentication allows only known SMs onto the network (blocking “rogue” SMs), and can be configured to ensure SMs are connecting to a known network (preventing SMs from connecting to “rogue” APs). RADIUS authentication is used for SMs, but is not used for APs, BHMs, or BHSs.

lternatively, through the use of Prizm Release 2.0 or later, or BAM Release 2.1 you can enhance network security by requiring SMs to authenticate when they register. Three keys and a random number are involved in authentication as follows:

- factory-set key in each SM. Neither the subscriber nor the network operator can view or change this key.
- authentication key, also known as authorization key and skey. This key matches in the SM and AP as the **Authentication Key** parameter, and in the Prizm database.
- random number, generated by Prizm or BAM and used in each attempt by an SM to register and authenticate. The network operator can view this number.
- session key, calculated separately by the SM and Prizm or BAM, based on both the authentication key (or, by default, the factory-set key) and the random number. Prizm or BAM sends the session key to the AP. The network operator cannot view this key.

None of the above keys is ever sent in an over-the-air link during an SM registration attempt. However, with the assumed security risk, the operator can create and configure the **Authentication Key** parameter.

Filtering Protocols and Ports

You can filter (block) specified protocols and ports from leaving the SM and entering the network. This protects the network from both intended and inadvertent packet loading or probing by network users. By keeping the specified protocols or ports off the network, this feature also provides a level of protection to users from each other.

Protocol and port filtering is set per SM. Except for filtering of SNMP ports, filtering occurs as packets leave the SM. If an SM is configured to filter SNMP, then SNMP packets are blocked from entering the SM and, thereby, from interacting with the SNMP portion of the protocol stack on the SM.

Port Filtering with NAT Enabled

Where NAT is enabled, you can filter only the three user-defined ports. The following are example situations in which you can configure port filtering where NAT is enabled.

- To block a subscriber from using FTP, you can filter Ports 20 and 21 (the FTP ports) for both the TCP and UDP protocols.
- To block a subscriber from access to SNMP, you can filter Ports 161 and 162 (the SNMP ports) for both the TCP and UDP protocols.
  NOTE: In only the SNMP case, filtering occurs before the packet interacts with the protocol stack.

Protocol and Port Filtering with NAT Disabled

Where NAT is disabled, you can filter both protocols and the three user-defined ports. Using the check boxes on the interface, you can either

- allow all protocols except those that you wish to block.
- block all protocols except those that you wish to allow.

You can allow or block any of the following protocols:

- PPPoE (Point to Point Protocol over Ethernet)
- Any or all of the following IPv4 (Internet Protocol version 4) protocols:
  - SMB (Network Neighborhood)
  - SNMP
  - Up to 3 user-defined ports
  - All other IPv4 traffic (see Figure 151)
- Uplink Broadcast
- ARP (Address Resolution Protocol)
- All others (see Figure 151)

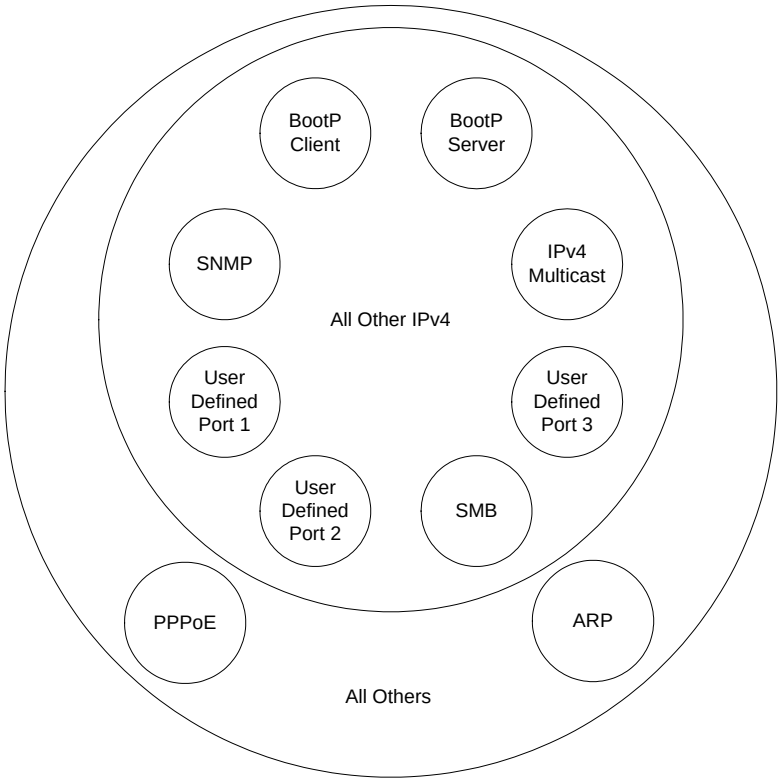


Figure 151: Categorical protocol filtering

The following are example situations in which you can configure protocol filtering where NAT is disabled:

- If you block a subscriber from only PPoE and SNMP, then the subscriber retains access to all other protocols and all ports.
- If you block PPoE, IPv4, and Uplink Broadcast, and you also check the **All others** selection, then only Address Resolution Protocol is not filtered.

The ports that are filtered as a result of protocol selections in the Protocol Filtering tab of the SM are listed in Table 63. Further information is provided under Protocol Filtering Tab of the SM on Page 317.

Table 63: Ports filtered per protocol selections

Protocol Selected	Port Filtered (Blocked)
SMB	Destination Ports 137 TCP and UDP, 138 UDP, 139 TCP, 445 TCP
SNMP	Destination Ports 161 TCP and UDP, 162 TCP and UDP
Bootp Client	Source Port 68 UDP
Bootp Server	Source Port 67 UDP

Encrypting Downlink Broadcasts

An AP can be enabled to encrypt downlink broadcast packets such as the following:

- ARP
- NetBIOS
- broadcast packets containing video data on UDP.

The encryption used is DES for a DES module, and AES for an AES module. Before the Encrypt Downlink Broadcast feature is enabled on the AP, air link security should be enabled on the AP.

Isolating SMs

In an AP, you can prevent SMs in the sector from directly communicating with each other. In CMMmicro Release 2.2 or later and the CMM4, you can prevent connected APs from directly communicating with each other, which prevents SMs that are in different sectors of a cluster from communicating with each other.

In the AP, the **SM Isolation** parameter is available in the General tab of the Configuration web page. In the drop-down menu for that parameter, you can configure the SM Isolation feature by any of the following selections:

- **Disable SM Isolation** (the default selection). This allows full communication between SMs.
- **Block SM Packets from being forwarded**. This prevents both multicast/broadcast and unicast SM-to-SM communication.
- **Block and Forward SM Packets to Backbone**. This not only prevents multicast/broadcast and unicast SM-to-SM communication but also sends the packets, which otherwise would have been handled SM to SM, through the Ethernet port of the AP.

In the CMMmicro and the CMM4, SM isolation treatment is the result of how you choose to manage the port-based VLAN feature of the embedded switch, where you can switch all traffic from any AP or BH to an uplink port that you specify. However, this is not packet level switching. It is not based on VLAN IDs. See the **VLAN Port Configuration** parameter in the dedicated user guide that supports the CMM product that you are deploying.

Filtering Management through Ethernet

You can configure the SM to disallow any device that is connected to its Ethernet port from accessing the IP address of the SM. If you set the **Ethernet Access Control** parameter to **Enabled**, then

- no attempt to access the SM management interface (by http, SNMP, telnet, ftp, or tftp) through Ethernet can succeed.
- any attempt to access the SM management interface over the air (by IP address, presuming that **LAN1 Network Interface Configuration, Network Accessibility** is set to **Public**, or by link from the Session Status or Remote Subscribers tab in the AP) is unaffected.

Allowing Management from Only Specified IP Addresses

The Security tab of the Configuration web page in the AP, SM, and BH includes the **IP Access Control** parameter. You can specify one, two, or three IP addresses that should be allowed to access the management interface (by http, SNMP, telnet, ftp, or tftp).

If you select

- **IP Access Filtering Disabled**, then management access is allowed from any IP address, even if the **Allowed Source IP *1 to 3*** parameters are populated.
- **IP Access Filtering Enabled**, and specify at least one address in the **Allowed Source IP *1 to 3*** parameter, then management access is limited to the specified address(es). If you intend to use Prizm to manage the element, then you must ensure that the IP address of the Prizm server is listed here.

Configuring Management IP by DHCP

The IP tab in the Configuration web page of every radio contains a **LAN1 Network Interface Configuration, DHCP State** parameter that, if enabled, causes the IP configuration (IP address, subnet mask, and gateway IP address) to be obtained through DHCP instead of the values of those individual parameters. The setting of this DHCP state parameter is also viewable, but is not settable, in the Network Interface tab of the Home page.

In the SM, this parameter is settable

- in the NAT tab of the Configuration web page, but only if NAT is enabled.
- in the IP tab of the Configuration web page, but only if the **Network Accessibility** parameter in the IP tab is set to **Public**.

Chapter 23: Managing Bandwidth and Authentication

This section provides a high-level description of bandwidth and authentication management in a network. For more specific information, see the *Cambium Canopy Prizm Release 3.2 User Guide*.

Managing Bandwidth without RADIUS, Prizm, or BAM

Unless RADIUS, Prizm or BAM is deployed and is configured in the AP, bandwidth management is limited to applying a single sustained data rate value (for uplink and for downlink) and a single burst allocation value (for uplink and for downlink) to every SM that registers in the AP.

Bandwidth and Authentication Manager (BAM) Services and Features

Prizm or BAM enables you to perform the following management operations on SMs:

- Change the key that the SMs need for authenticating.
- Temporarily suspend or reinstate a subscriber.
- Set burst size and data transfer rate caps for an SM or group of SMs.
- Use licensing to uncap an SM or group of SMs.
- List all ESNs that are associated with a specified VLAN ID.
- Associate or dissociate an SM or group of SMs with a specified VLAN ID.
- Set VLAN parameters.
- Toggle whether to send those VLAN parameters to the SMs.
- Set CIR parameters for low-priority and high-priority channel rates.
- Toggle whether to send those CIR parameters to the SMs.
- Toggle whether to enable the high-priority channel in the SMs.

Bandwidth Manager Capability

Prizm or BAM allows you to set bandwidth per SM for sustained rates and burst rates. With this capability, the system allows both

- burst rates beyond those of many other broadband access solutions.
- control of average bandwidth allocation to prevent excessive bandwidth usage by a subscriber.

All packet throttling occurs in the SMs and APs based on Quality of Service (QoS) data that the Prizm or BAM server provides. No server processing power or network messages are needed for packet throttling.

QoS management also supports marketing of broadband connections at various data rates, for operator-defined groups of subscribers, and at various price points. This allows you to meet customer needs at a price that the customer deems reasonable and affordable.

When **Authentication Server** *is* selected in the Security tab of the AP Configuration web page and one or more **Authentication Server** is specified by IP address, bandwidth management is expanded to apply uniquely specified sustained data rate and burst allocation values to each SM registered in the AP. So, you can define differently priced tiers of subscriber service.

Designing Tiered Subscriber Service Levels

Examples of levels of service that vary by bandwidth capability are provided in Table 64 and Table 65.

NOTE:
The speeds that these tables correlate to service levels are comparative examples. Actual download times may be greater due to use of the bandwidth by other SMs, congestion on the local network, congestion on the Internet, capacity of the serving computer, or other network limitations.

Table 64: Example times to download for typical tiers of service with CAP 120

Equipment	**AP**	**CAP 120**		
	SM	**CSM 120**		
	Operation	**1X**		
	Max burst speed	**4.4 Mbps**		
Example Settings	**Service Type**	Premium	Regular	Basic
	Sustained Downlink Data Rate	5250 Kbps	1000 Kbps	256 Kbps
	Sustained Uplink Data Rate	1750 Kbps	500 Kbps	128 Kbps

	Downlink and Uplink Burst Allocations	500000 Kb	80000 Kb	40000 Kb
Download (sec)	**Web page**	<1	<1	<1
	5 MB	9	9	9
	20 MB	36	80	470
	50 MB	91	320	1400
	300 MB	545	2320	9220

Table 65: Example times to download for typical tiers of service with CAP 130

Equipment	**AP**	**CAP 130**						
	SM	**CSM 130**						
	Operation	**1X**			**2X**			**2X**
	Max burst speed	**5 Mbps**			**10 Mbps**			**10 Mbps**
Example Settings	**Service Type**	Premium	Regular	Basic	Premium	Regular	Basic	Premium
	Sustained Downlink Data Rate	5250 Kbps	1000 Kbps	256 Kbps	5250 Kbps	1000 Kbps	256 Kbps	2000 Kbps
	Sustained Uplink Data Rate	1750 Kbps	500 Kbps	128 Kbps	1750 Kbps	500 Kbps	128 Kbps	20000 Kbps
	Downlink and Uplink Burst Allocations	500000 Kb	80000 Kb	40000 Kb	500000 Kb	80000 Kb	40000 Kb	500000 Kb
Download (sec)	**Web page**	<1	<1	<1	<1	<1	<1	<1
	5 MB	8	8	8	4	4	4	4
	20 MB	32	80	470	16	80	470	16
	50 MB	80	320	1400	40	320	1400	40
	300 MB	480	2320	9220	362	2320	9220	240

Authentication Manager Capability

Prizm or BAM allows you to set per AP a requirement that each SM registering to the AP must authenticate. When **Authentication Server** *is* selected in the Security tab of the AP Configuration web page and one or more **Authentication Server** is specified by IP address, any SM that attempts to register to the AP is denied service if authentication fails, such as (but not limited to) when no Prizm or BAM server is operating or when the SM is not listed in the database.

If a Prizm or BAM server drops out of service where no redundant server exists

- an SM that attempts to register is denied service.
- an SM that is already in session remains in session

In a typical network, some SMs re-register daily (when subscribers power down the SMs, for example), and others do not re-register in a period of several weeks. Whenever an authentication attempt fails, the SM locks out of any other attempt to register itself to the same AP for the next 15 minutes.

Chapter 24: Configuring a RADIUS server

Configuring a RADIUS server in a PMP network is optional, but can provide added security, increase ease of network management and provide usage-based billing data.

Understanding RADIUS

RADIUS Functions

RADIUS protocol support provides the following functions:

- **SM Authentication** allows only known SMs onto the network (blocking "rogue" SMs), and can be configured to ensure SMs are connecting to a known network (preventing SMs from connecting to "rogue" APs). RADIUS authentication is used for SMs, but is not used for APs.
- **SM Configuration:** Configures authenticated SMs with MIR (Maximum Information Rate), High Priority, and VLAN (Virtual LAN) parameters from the RADIUS server when an SM registers to an AP.
- **Centralized AP and SM user name and password management** allows AP and SM usernames and access levels (Administrator, Installer, Technician) to be centrally administered in the RADIUS server instead of on each radio and tracks access events (logon/logoff) for each username on the RADIUS server. This accounting does *not* track and report specific configuration actions performed on radios or pull statistics such as bit counts from the radios. Such functions require an Element Management System (EMS) such as Cambium Networks Wireless Manager. This accounting is *not* the ability to perform accounting functions on the subscriber/end user/customer account.
- **Framed IP** allows operators to use a RADIUS server to assign management IP addressing to SM modules (framed IP address).

Tested RADIUS Servers

The Canopy RADIUS implementation has been tested and is supported on

- FreeRADIUS, Version 2.1.8
- Aradial RADIUS, Version 5.1.12

NOTE

Note, Aradial 5.3 has a bug that prevents “remote device login”, preventing usage of the user name and password management features.

Choosing Authentication Mode and Configuring for Authentication Servers - AP

On the AP’s Configuration > Security tab, select the **RADIUS AAA Authentication Mode**. The following describes the other **Authentication Mode** options for reference, and then the **RADIUS AAA** option.

- **Disabled:** Requires no authentication. Any SM (except an SM that itself has been configured to *require* RADIUS authentication by enabling Enforce Authentication as described below) will be allowed to register to the AP.
- **Authentication Server:** Authentication Server in this instance refers to Wireless Manager in BAM-only mode. Authentication will be required for an SM to register to the AP. Only SMs listed by MAC address in the Wireless Manager database will be allowed to register to the AP.
- **AP Pre-Shared Key:** Canopy offers a pre-shared key authentication option. In this case, an identical key must be entered in the Authentication Key field on the AP’s Configuration > Security tab and in the Authentication Key field on each desired SM’s Configuration > Security tab.
- **RADIUS AAA:** To support RADIUS authentication of SMs, on the AP’s Configuration > Security tab select RADIUS AAA. Only properly configured SMs with a valid certificate will be allowed to register to the AP.

When RADIUS AAA is selected, up to 3 Authentication Server (RADIUS Server) IP addresses and Shared Secrets can be configured. The IP address(es) configured here must match the IP address(es) of the RADIUS server(s). The shared secret(s) configured here must match the shared secret(s) configured in the RADIUS server(s). Servers 2 and 3 are meant for backup and reliability, not splitting the database. If Server 1 doesn’t respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, the SM is denied entry to the network, and does not progress trying the other servers.

The default IP address is 0.0.0.0. The default Shared Secret is “CanopySharedSecret”. The Shared Secret can be up to 32 ASCII characters (no diacritical marks or ligatures, for example)

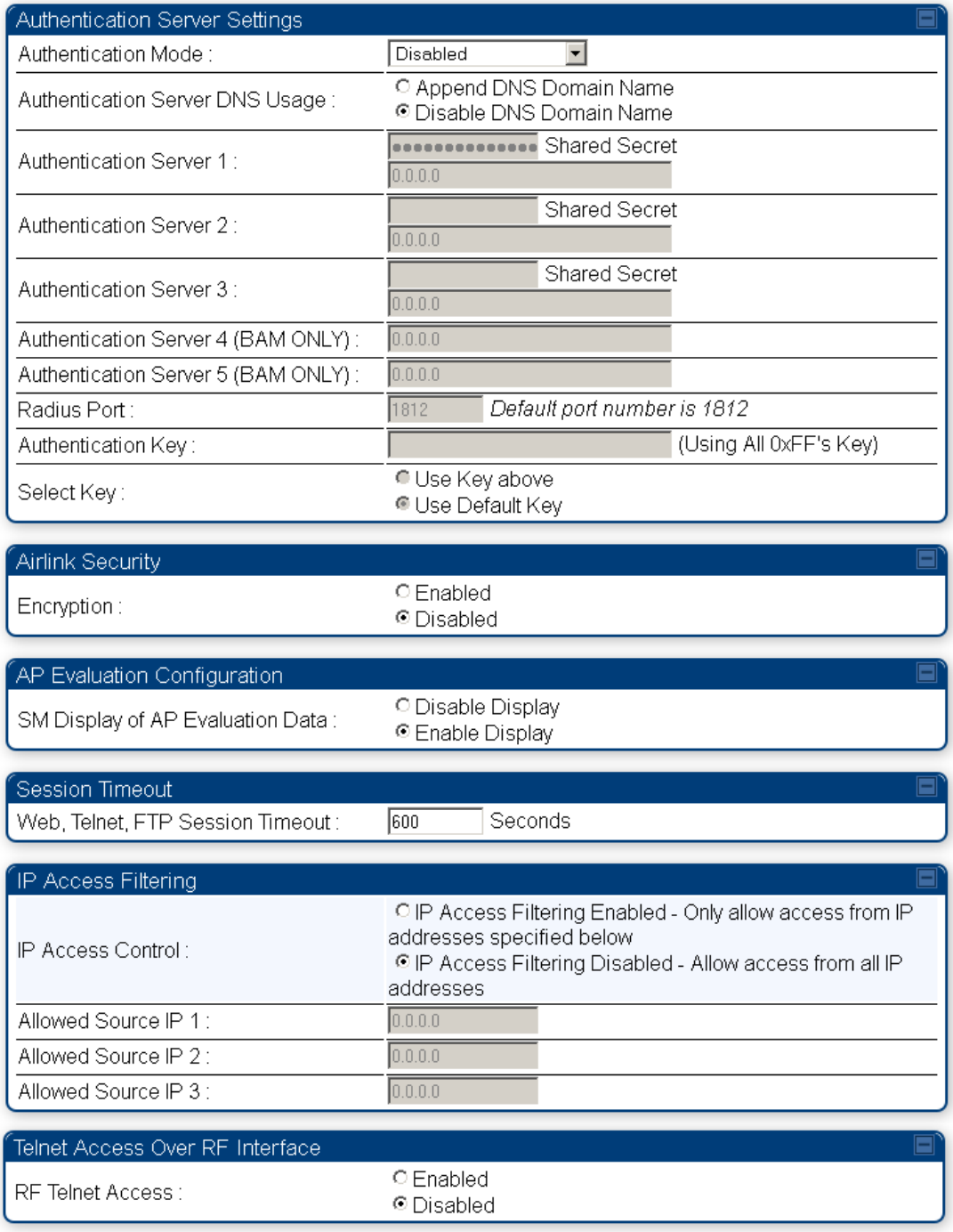


Figure 152: Security tab of the AP

SM Authentication Mode – Require RADIUS or Follow AP

If it is desired that an SM will only authenticate to an AP that is using RADIUS, on the SM's Configuration Security tab set **Enforce Authentication** to **AAA**. With this enabled, an SM will not register to an AP that has any **Authentication Mode** other than **RADIUS AAA** selected**.**

If it is desired that an SM use the authentication method configured on the AP it is registering to, set **Enforce Authentication** to **Disabled.** With **Enforce Authentication** disabled, an SM will attempt to register using whichever **Authentication Mode** is configured on the AP it is attempting to register to.

Note, requiring SMs to use RADIUS by enabling **Enforce Authentication** avoids the security issue of SMs possibly registering to "rogue" APs which have authentication disabled.

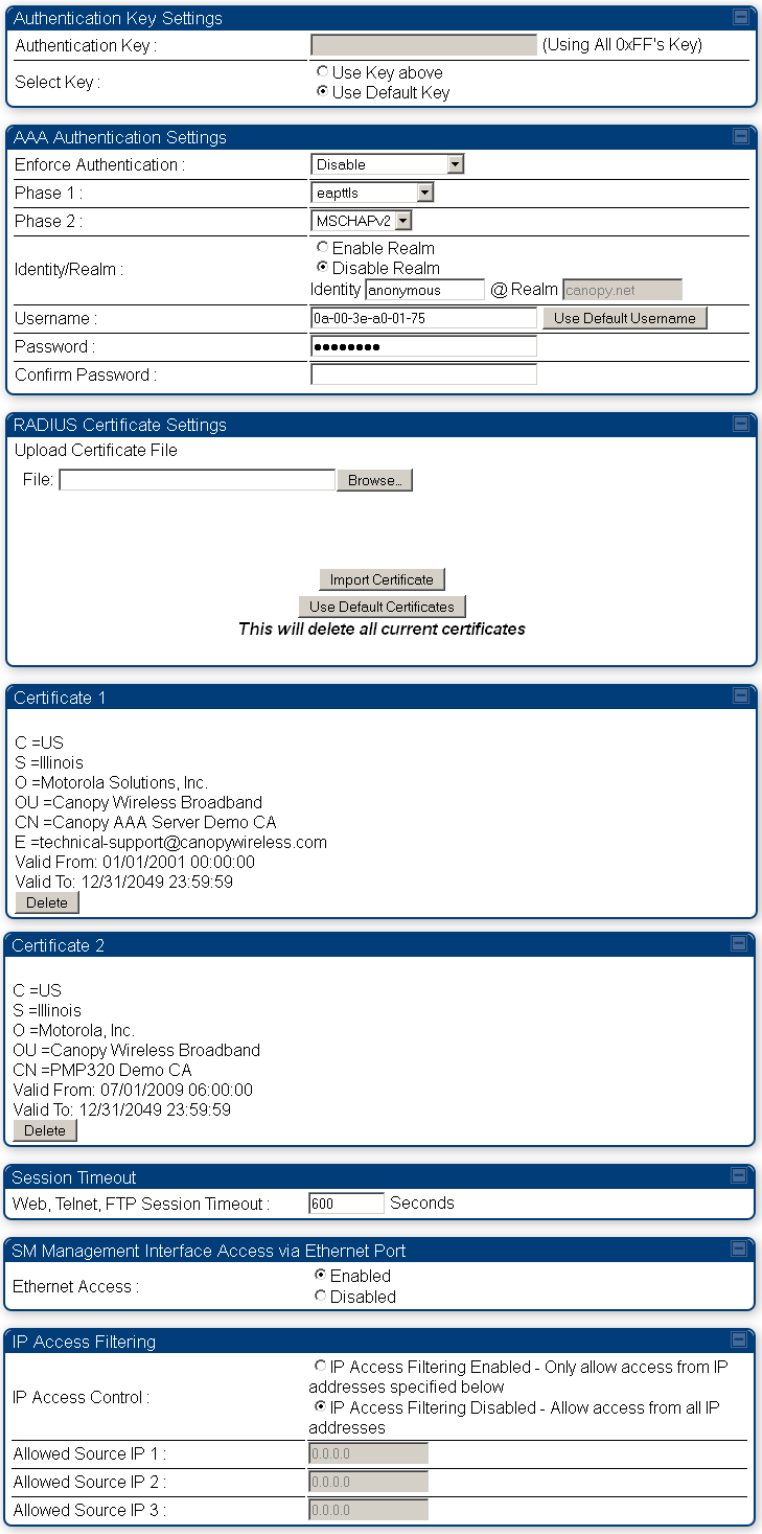


Figure 153: Security tab of the SM

SM - Phase 1 (Outside Identity) parameters and settings

The protocols supported for the **Phase 1** (Outside Identity) phase of authentication are

eapttls (Extensible Authentication Protocol Tunneled Transport Layer Security) and **eapMSChapV2** (Extensible Authentication Protocol – Microsoft Challenge-Handshake Authentication Protocol).

Configure an outer Identity in the **Username** field. This must match the Phase 1/Outer Identity username configured in the RADIUS server. The default Phase 1/Outer Identity **Username** is “anonymous”. The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters. If Realms are being used in the RADIUS system (**eapttls** only), select **Enable Realm** and configure an outer identity in the **Identity** field and a Realm in the **Realm** field. These must match the Phase 1/Outer Identity and Realm configured in the RADIUS server. The default **Identity** is “anonymous”. The **Identity** can be up to 128 non-special (no diacritical markings) alphanumeric characters. The default **Realm** is “canopy.net”. The **Realm** can also be up to 128 non-special alphanumeric characters.

SM - Phase 2 (Inside Identity) parameters and settings

If using **eapttls** for Phase 1 authentication, select the desired **Phase 2** (Inside Identity) authentication protocol from the **Phase 2** options of **PAP** (Password Authentication Protocol), **CHAP** (Challenge Handshake Authentication Protocol), and **MSCHAPv2 (**Microsoft’s version of CHAP). The protocol must be consistent with the authentication protocol configured on the RADIUS server. Enter a **Username** for the SM. This must match the username configured for the SM on the RADIUS server. The default **Username** is the SM’s MAC address. The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.

Enter the desired password for the SM in the **Password** and **Confirm Password** fields**..** The **Password** must match the password configured for the SM on the RADIUS server. The default **Password** is “password”. The **Password** can be up to 128 non-special (no diacritical markings) alphanumeric characters.

Handling Certificates

Managing SM Certificates via the SM GUI

The default public Canopy certificates are loaded into SMs upon factory software installation. The default certificates are not secure and are intended for use during lab and field trials as part of gaining experience with the RADIUS functionalities or as an option during debug. For secure operation, an operator will want to create or procure their own certificates.

Up to 2 certificates can be resident on an SM. An installed certificate can be deleted by clicking the **Delete** button in the certificate's description block on the Configuration > Security tab. To restore fhe 2 default certificates, click the **Use Default Certificates** button in the **RADIUS Certificate Settings** parameter block and reboot the radio.

To upload a certificate manually to an SM, first load it in a known place on your PC or network drive, then click on a **Delete** button on one of the Certificate description blocks to delete a certificate to provide space for your certificate. Click on **Choose File,** browse to the location of the certificate, and click the **Import Certificate** button, and then reboot the radio to use the new certificate.

When a certificate is in use, after the SM successfully registers to an AP, an indication of **In Use** will appear in the description block of the certificate being used.

The public certificates installed on the SMs are used with the private certificate on the RADIUS server to provide a public/private key encryption system.

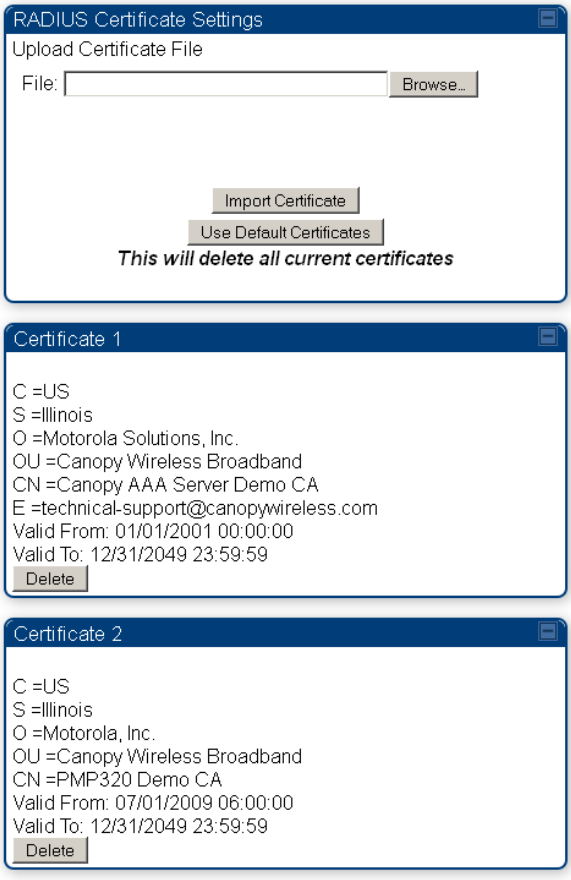


Figure 154: SM Certificate Management

Configuring your RADIUS servers for SM authentication

Your RADIUS server will need to be configured to use the following:

- EAPTTLS or MSCHAPv2 as the Phase 1/Outer Identity protocol.
- If **Enable Realm** is selected on the SM's **Configuration** > **Security** tab, then the same Realm as appears there (or access to it).
- The same Phase 2 (Inner Identity) protocol as configured on the SM's **Configuration > Security** tab under Phase 2 options.
- The username and password for each SM configured on each SM's Configuration > Security tab.
- An IP address and NAS shared secret that is the same as the IP address and **Shared Secret** configured on the AP's Configuration > Security tab for that RADIUS server.
- A server private certificate, server key, and CA certificate that complement the public certificates distributed to the SMs, as well as the Canopy dictionary file that defines Vendor Specific Attributes (VSAa). Default certificate files and the dictionary file are available from the software site: www.cambiumnetworks.com/support/pmp/software/ after entering your name, email address, and either Customer Contract Number or the MAC address of a module covered under the 12 month warranty.

Optionally, operators may configure the RADIUS server response messages (Accept or Reject) so that the user has information as to why they have been rejected. The AP displays the RADIUS Authentication Reply message strings in the Session Status list as part of each SM's information. The SM will show this string (listed as Authentication Response on the SM GUI)on the main Status page in the Subscriber Module Stats section.

(Note: Aradial AAA servers only support operator-configurable Authentication Accept responses, not Authentication Reject responses).

Configuring your RADIUS server for SM configuration

Table 66 lists Canopy Vendor Specific Attributes (VSAs) along with VSA numbers and other details. The associated SM GUI page, tab, and parameter is listed to aid cross-referencing and understanding of the VSAs.

A RADIUS dictionary file is available from the software site: www.cambiumnetworks.com/support/pmp/software/

The RADIUS dictionary file defines the VSAs and their values and is usually imported into the RADIUS server as part of server and database setup.

Assigning SM management IP addressing via RADIUS

Operators may use a RADIUS AAA server to assign management IP addressing to SM modules (framed IP address). SMs now interpret attributes Framed-IP-Address, Framed-IP-Netmask, and Cambium-Canopy-Gateway from RADIUS. The RADIUS dictionary file has been updated to include the Cambium-Canopy-Gateway attribute and is available on the Cambium Software Support website.

In order for these attributes to be assigned and used by the SM, the following must be true:

- The Canopy system is configured for AAA authentication
- The SM is *not* configured for DHCP on its management interface. If DHCP is enabled and these attributes are configured in the RADIUS server, the attributes will be ignored by the SM.
- The SM management interface must be configured to be publically accessible. If the SM is configured to have local accessibility, the management interface will still be assigned the framed addressing, and the SM will become publicly accessible via the assigned framed IP addressing.
- When using these attributes, for the addressing to be implemented by the SM operators must configure Framed-IP-Address in RADIUS. If Framed-IP-Address is not configured but Framed-IP-Netmask and/or Cambium-Canopy-Gateway is configured, the attributes will be ignored. In the case where only the Framed-IP-Address is configured, Framed-IP-Netmask defaults to 255.255.0.0 (NAT disabled) / 255.255.255.0 (NAT enabled) and Cambium-Canopy-Gateway defaults to 0.0.0.0.

Table 66 RADIUS Vendor Specific Attributes (VSAs)

Name	Number	Type	Req'd	Value	
SM GUI Page > Tab > Parameter				Default	Size
MS-MPPE-Send-Key	26.311.16	-	Y	-	
-				-	-
MS-MPPE-Recv-Key	26.311.17	-	Y	-	
-				-	-

Cambium-Canopy-HPENABLE	26.161.5	integer	N	0-disable, 1-enable	
Configuration > Quality of Service > Hi Priority Channel				0	32 bits
Cambium-Canopy-ULBR	26.161.6	integer	N	0-50000+ kbps	
Configuration > Quality of Service > Sustained Uplink Data Rate				dependent on radio feature set	32 bits
Cambium-Canopy-ULBL	26.161.7	integer	N	0-50000+ kbps	
Configuration > Quality of Service > Uplink Burst Allocation				dependent on radio feature set	32 bits
Cambium-Canopy-DLBR	26.161.8	integer	N	0-50000+ kbps	
Configuration > Quality of Service > Sustained Downlink Data Rate				dependent on radio feature set	32 bits
Cambium-Canopy-DLBL	26.161.9	integer	N	0-50000+ kbps	
Configuration > Quality of Service > Downlink Burst Allocation				dependent on radio feature set	32 bits
Cambium-Canopy-	26.161.14	integer	N	0-disable, 1-enable	
Configuration > VLAN > Dynamic Learning				1	32 bits
Cambium-Canopy-VLFRAMES	26.161.15	integer	N	0-all, 1-tagged, 2-untagged	
Configuration > VLAN > Allow Frame Types				0	32 bits
Cambium-Canopy-VLIDSET	26.161.16	integer	N	VLAN Membership (1-4094)	
Configuration > VLAN Membership				0	32 bits
Cambium-Canopy-VLAGETO	26.161.20	integer	N	5 - 1440 minutes	
Configuration > VLAN > VLAN Aging Timeout				25 mins	32 bits
Cambium-Canopy-VLIGVID	26.161.21	integer	N	1 – 4094	
Configuration > VLAN > Default Port VID				1	32 bits
Cambium-Canopy-VLMGVID	26.161.22	integer	N	1 – 4094	
Configuration > VLAN > Management VID				1	32 bits
Cambium-Canopy-VLSMMGPASS	26.161.23	integer	N	0-disable, 1-enable	
Configuration > VLAN > SM Management VID Pass-through				1	32 bits
Cambium-Canopy-BCASTMIR	26.161.24	integer	N	0-50000+ kbps, 0=disabled	
Configuration > Quality of Service > Broadcast/Multicast Uplink Data Rate				dependent on radio feature set	32 bits
Cambium-Canopy-Gateway	26.161.25	ipaddr	N	-	
Configuration > IP > Gateway IP Address				0.0.0.0	-

Cambium-Canopy-UserLevel	26.161.50	integer	N	1-Technician, 2-Installer, 3-Administrator	
Account > Add User > Level				0	32 bits
Note about VSA numbering: 26 connotes Vendor Specific Attribute, per RFC 2865 26.311 is Microsoft Vendor Code, per IANA					

Using RADIUS for centralized AP and SM user name and password management

AP – Technician/Installer/Administrator Authentication

To control technician, installer, and administrator access to the AP from a centralized RADIUS server:

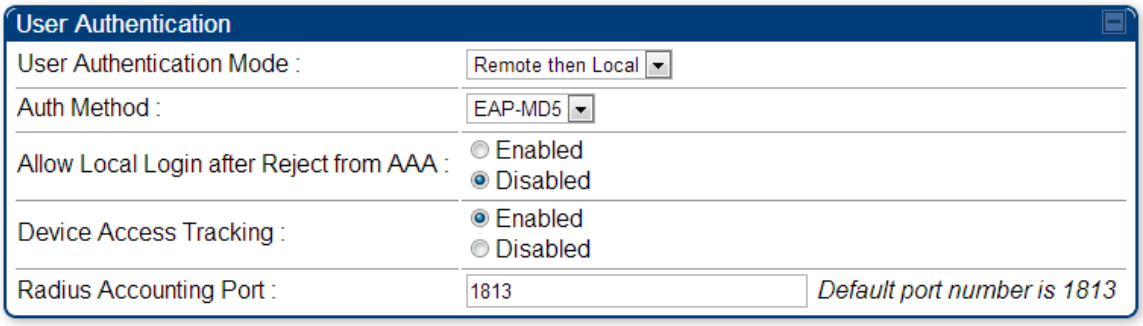
1. Set **Authentication Mode** on the AP's Configuration > Security tab to **RADIUS AAA**
2. Set **User Authentication Mode** on the AP's Account > User Authentication tab (the tab only appears after the AP is set to RADIUS authentication) to **Remote** or **Remote then Local**.
   - **Local**: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed.
   - **Remote**: Authentication by the centralized RADIUS server is required to gain access to the SM if the SM is registered to an AP that has **RADIUS AAA Authentication Mode** selected. For up to 2 minutes a test pattern will be displayed until the server responds or times out.
   - **Remote then Local**: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the SM.

Either the same RADIUS server used for SM authentication can be used for user authentication and accounting (access control), or a separate RADIUS accounting server can be used. Indicate your network design under **Authentication Server Settings** in the AP's **Security** tab.

If separate accounting server(s) are used, configure the IP address(es) and **Shared Secret**(s) in the **Accounting Server** fields. The default **Shared Secret** is "CanopyAcctSecret". Up to 3 servers can be used for redundancy. Servers 2 and 3 are meant for backup and reliability, not

splitting the database. If Server 1 doesn't respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, Server 2 is not tried.

Figure 155 User Authentication tab of the AP



SM – Technician/Installer/Administrator Authentication

To control technician, installer, and administrator access to the SM from a centralized RADIUS server:

1. Set **Authentication Mode** on the AP's Configuration > Security tab to **RADIUS AAA** (RADIUS)
2. Set **User Authentication Mode** on the AP's Account > User Authentication tab (the tab only appears after the AP is set to AAA authentication) to **Remote** or **Remote then Local**.
3. Set **User Authentication Mode** on the SM's Account > User Authentication tab to **Remote** or **Remote then Local**.
    - **Local**: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed.
    - **Remote**: Authentication by the centralized RADIUS server is required to gain access to the SM if the SM is registered to an AP that has **RADIUS AAA Authentication Mode** selected. For up to 2 minutes a test pattern will be displayed until the server responds or times out.
    - **Remote then Local**: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the SM.

Note, remote access control is enabled only after the SM registers to an AP that has **Authentication Mode** set to **RADIUS AAA**. Local access control will always be used before registration and will be used after registration if the AP is not configured for RADIUS.

Figure 156 User Authentication tab of the AP

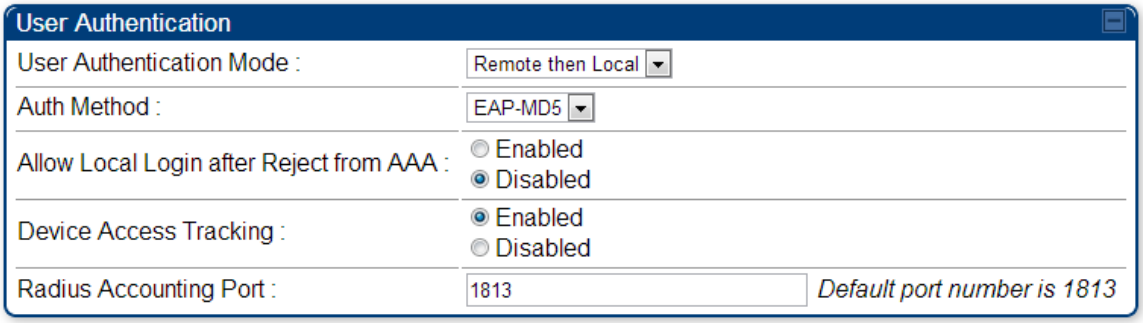


Table 67: AP User Authentication attributes

Attribute	Meaning
User Authentication Mode	• **Local**: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed. • **Remote**: Authentication by the centralized RADIUS server is required to gain access to the AP. For up to 2 minutes a test pattern will be displayed until the server responds or times out. • **Remote then Local**: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the AP.
Auth Method	The user authentication method employed by the radios is EAP-MD5.
Allow Local Login after Reject from AAA	If a user authentication is rejected from the AAA server, the user will be allowed to login locally to the radio's management interface.
Device Access Tracking	To track logon and logoff times on individual radios by technicians, installers, and administrators, set this parameter to **Enabled**.
Radius Accounting Port	The destination port on the AAA server used for Radius accounting communication.

Figure 157 User Authentication tab of the SM

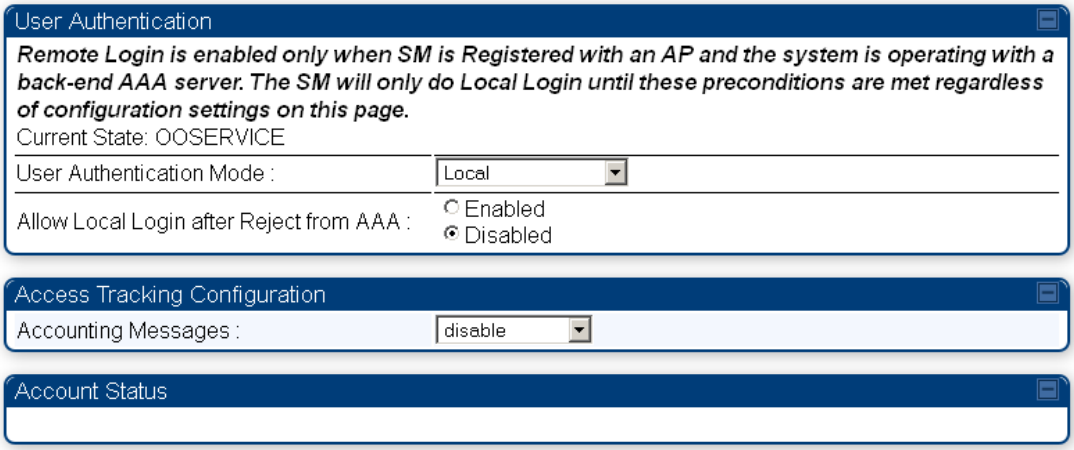

User Authentication
Remote Login is enabled only when SM is Registered with an AP and the system is operating with a back-end AAA server. The SM will only do Local Login until these preconditions are met regardless of configuration settings on this page.
Current State: OOSERVICE
User Authentication Mode :
Local
Allow Local Login after Reject from AAA :
Enabled
Disabled
Access Tracking Configuration
Accounting Messages :
disable
Account Status

Table 68: SM User Authentication attributes

Attribute	Meaning
User Authentication Mode	• **Local**: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed. • **Remote**: Authentication by the centralized RADIUS server is required to gain access to the SM if the SM is registered to an AP that has **RADIUS AAA Authentication Mode** selected. For up to 2 minutes a test pattern will be displayed until the server responds or times out. • **Remote then Local**: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the SM.
Allow Local Login after Reject from AAA	If a user authentication is rejected from the AAA server, the user will be allowed to login locally to the radio's management interface.
Accounting Messages	• disable – no accounting messages are sent to the RADIUS server • deviceAccess – accounting messages are sent to the RADIUS server regarding device access

Access Tracking

To track logon and logoff times on individual radios by technicians, installers, and administrators, on the AP or SM's **Account** > **User Authentication** tab under **Accounting** (Access Tracking) set **Accounting Messages** to "deviceAccess".

Device Access Tracking is enabled separately from **User Authentication Mode**. A given AP or SM can be configured for both, either, or neither.

RADIUS Attribute Framed-IP-Address

Operators may now use a RADIUS AAA server to assign management IP addressing to SM modules (framed IP address). SMs now interpret attributes Framed-IP-Address, Framed-IP-Netmask, and Cambium-Gateway from RADIUS. The RADIUS dictionary file has been updated to include the Cambium-Gateway attribute and is available on the Cambium Software Support website.

In order for these attributes to be assigned and used by the SM, the following must be true:

- The Canopy system is configured for AAA authentication
- The SM is *not* configured for DHCP on its management interface. If DHCP is enabled and these attributes are configured in the RADIUS server, the attributes will be ignored by the SM.
- The SM management interface must be configured to be publically accessible. If the SM is configured to have local accessibility, the management interface will still be assigned the framed addressing, and the SM will become publicly accessible via the assigned framed IP addressing.

When using these attributes, for the addressing to be implemented by the SM operators must configure Framed-IP-Address in RADIUS. If Framed-IP-Address is not configured but Framed-IP-Netmask and/or Cambium-Gateway is configured, the attributes will be ignored. In the case where only the Framed-IP-Address is configured, Framed-IP-Netmask defaults to 255.255.0.0 (NAT disabled) / 255.255.255.0 (NAT enabled) and Cambium-Gateway defaults to 0.0.0.0

Chapter 25: Managing the Network From a Management Station (NMS)

SNMPv2 (Simple Network Management Protocol Version 2) can be used to manage and monitor the modules under SMI (Structure of Management Information) specifications. SMI specifies management information definitions in ASN.1 (Abstract Syntax Notation One) language. SNMPv2 supports both 32-bit and 64-bit counters. The SMI for SNMPv2 is defined in RFC 1902 at http://www.faqs.org/rfcs/rfc1902.html.

Roles of Hardware and Software Elements

Role of the Agent

In SNMP, software on each managed device acts as the *agent*. The agent collects and stores management information in ASN.1 format, in a structure that a MIB (management information base) defines. The agent responds to commands to

- send information about the managed device.
- modify specific data on the managed device.

Role of the Managed Device

In SNMP, the managed device is the network element that operates on the agent software. In the fixed wireless broadband IP network, this managed device is the module (AP, SM, or BH). With the agent software, the managed device has the role of server in the context of network management.

Role of the NMS

In SNMP, the NMS (network management station) has the role of client. An application (manager software) operates on the NMS to manage and monitor the modules in the network through interface with the agents.

Dual Roles for the NMS

The NMS can simultaneously act as an agent. In such an implementation, the NMS acts as

- client to the agents in the modules, when polling for the agents for information and sending modification data to the agents.
- server to another NMS, when being polled for information gathered from the agents and receiving modification data to send to the agents.

Simple Network Management Protocol (SNMP) Commands

To manage a module, SNMPv2 supports the `set` command, which instructs the agent to change the data that manages the module.

To monitor a network element, SNMPv2 supports

- the `get` command, which instructs the agent to send information about the module to the manager in the NMS.
- traversal operations, which the manager uses to identify supported objects and to format information about those objects into relational tables.

In a typical network, the manager issues these commands to the agents of more than one module (to all SMs in the operator network, for example).

Traps from the Agent

When a specified event occurs in the module, the agent initiates a trap, for which the agent sends an unsolicited asynchronous message to the manager.

AP SNMP Proxy to SMs

When the AP receives from Prizm or an NMS an SNMP request for an SM, it is capable of sending that request via proxy to the SM. In this case, the SM responds directly to Prizm or the NMS. (The AP performs no processing on the response.)

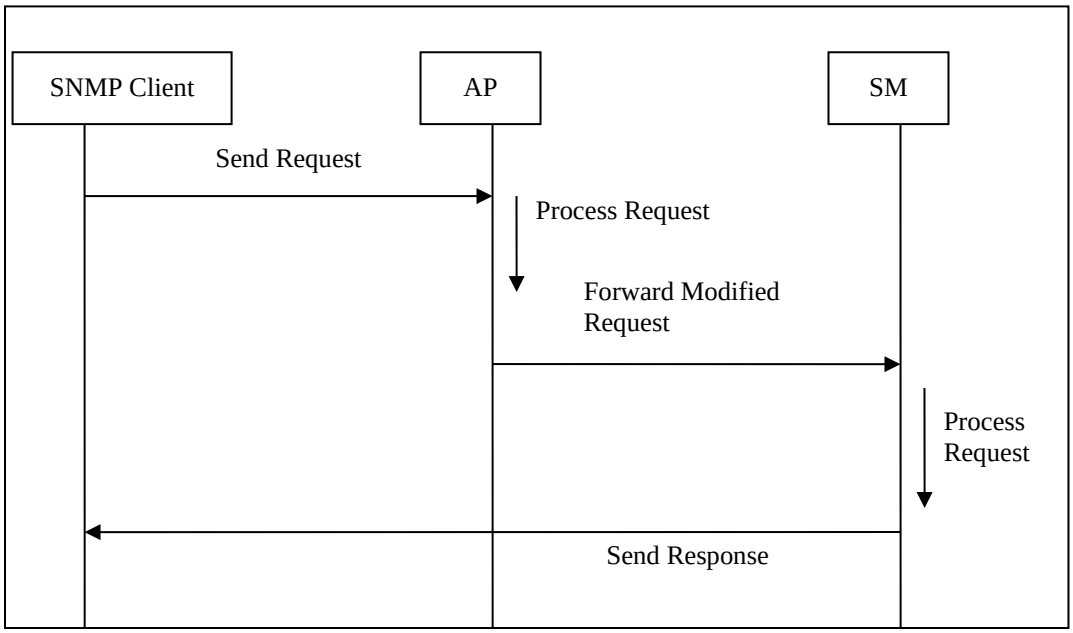


Table 69: SNMP Proxy flow

Configuration of Slave Devices

The Slave Devices should be configured with a local IP address with the appropriate gateway setup.

The IP Configurations of the System should be such that the slave Ethernet interface and the SNMP Client are not on the same subnet. This scenario will cause all traffic from the slave devices to the SNMP Client to be sent out via its Ethernet interface, preventing routing back to the SNMP Client.

SNMP Proxy UDP Port

The SNMP Proxy is listening for SNMP requests to forward on UDP port 61002. It forwards the request to the slave device (SM or BHS) using UDP port 161.

Packet Format

The first OID sent in an SNMP request needs be modified to include the MAC address of the slave device The remaining OIDs will remain the same as slave OIDs:

.SlaveOID. <MAC>
.SlaveOID
.SlaveOID

<MAC> = the MAC Address of the Registered Slave Device to which the request needs to be forwarded by the SNMP Proxy. Each byte of the MAC Address is encoded as a separate integer. Thus the MAC will contain the information for 6 integers:

SlaveOID = the OID to query in the Slave device. This is the actual OID that is implemented within the MIB of the slave device.

SNMP Proxy Example - Get

SM MAC: 0a-00-3e-a0-00-a5; Converted to decimal: 10.0.62.160.0.165
AP IP: 10.120.153.6
Community String: Canopy

OID: whispSMConfig rFScanList .1.3.6.1.4.1.161.19.3.2.1.1.0

```
snmpget -p 61002 -v 2 -c Canopy 10.120.153.6
.1.3.6.1.4.1.161.19.3.2.1.1.0.10.0.62.160.0.165
```

This returns:

```
.1.3.6.1.4.1.161.19.3.2.1.1.0
Value (OctetString): 547500, 548000, 548500, 549000, 549500, 550000,
550500, 551000, 551500, 552000
```

SNMP Proxy Example - Get Multiple OIDs

This example uses the same AP and SM as above.

OIDs: whispSMStatus radioDbm .1.3.6.1.4.1.161.19.3.2.2.8.0
whispSMStatus registeredToAp .1.3.6.1.4.1.161.19.3.2.2.9.0
whispSMStatus adaptRate .1.3.6.1.4.1.161.19.3.2.2.20.0

```
snmpget -p 61002 -v 2 -c Canopy 10.120.153.6
.1.3.6.1.4.1.161.19.3.2.2.8.0.10.0.62.160.0.165
1.3.6.1.4.1.161.19.3.2.2.9.0 .1.3.6.1.4.1.161.19.3.2.2.20.0
Value (OctetString): -53.6

.1.3.6.1.4.1.161.19.3.2.2.9.0
Value (OctetString): 0a-00-3e-a0-07-7c

.1.3.6.1.4.1.161.19.3.2.2.20.0
Value (OctetString): VC  18 Rate 6X/4X    VC 255 Rate 6X/1X
```

SNMP Proxy Example - Set

Note: For SNMP writes to work, the SNMP Community String 1 Permissions must be set to Read / Write.

OID: whispSMConfig lanIpSm .1.3.6.1.4.1.161.19.3.2.1.3.0

```
snmpset -p 61002 -v 2 -c Canopy 10.120.153.6
.1.3.6.1.4.1.161.19.3.2.1.3.0.10.0.62.160.0.165 a 169.254.1.2
.1.3.6.1.4.1.161.19.3.2.1.3.0
Value (IpAddress): 169.254.1.2
```

SNMP Trap Notification for Slave Devices

The SNMP Proxy will not forward traps. The Slave devices must be configured to send traps directly to the SNMP Trap Receiver.

SNMP Proxy Errors - Other

If there is an error there will not be a response sent back to the SNMP agent. Possible errors include:

- Community String incorrect
- SM with that MAC address is not registered to that AP
- SNMP Read / Write is not enabled
- OID incorrect

Management Information Base (MIB)

The MIB, the SNMP-defined data structure, is a tree of standard branches that lead to optional, non-standard positions in the data hierarchy. The MIB contains both

- objects that SNMP is allowed to control (bandwidth allocation or access, for example)
- objects that SNMP is allowed to monitor (packet transfer, bit rate, and error data, for example).

The path to each object in the MIB is unique to the object. The endpoint of the path is the object identifier.

Cascading Path to the MIB

The standard MIB hierarchy includes the following cascading branch structures:

- the top (standard body) level:
  - ccitt (0)
  - **iso (1)**
  - iso-ccitt (2)

- under iso (1) above:
  - standard (0)
  - registration-authority (1)
  - member-body (2)
  - **identified-organization (3)**
- under identified-organization (3) above:
  - dod (6)
  - other branches
- under dod (6) above:
  - internet (1)
  - other branches
- under internet (1) above:
  - mgmt (2)
  - private (4)
  - other branches
- under mgmt (2) above: **mib-2 (1)** and other branches. (See MIB-II below.)
- under private (4) above: enterprise (1) and other branches. (See Canopy Enterprise MIB below.)

Beneath this level are non-standard branches that the enterprise may define.

Thus, the path to an object that is managed under MIB-II begins with the decimal string **1.3.6.1.2.1** and ends with the object identifier and instance(s), and the path to an object that is managed under the Canopy Enterprise MIB begins with **1.3.6.1.4.1**, and ends with the object identifier and instance(s).

Object Instances

An object in the MIB can have either only a single instance or multiple instances, as follows:

- a scalar object has only a single instance. A reference to this instance is designated by `.0`, following the object identifier.
- a tabular object has multiple instances that are related to each other. Tables in the MIB associate these instances. References to these instances typically are designated by `.1`, `.2`, and so forth, following the object identifier.

Management Information Base Systems and Interface (MIB-II)

The standard MIB-II (Management Information Base systems and interface) objects are programmed into the modules. To read this MIB, see *Management Information Base for Network Management of TCP/IP-based Internets: MIB II*, RFC 1213 at http://www.faqs.org/rfcs/rfc1213.html.

The MIB-II standard categorizes each object as one of the types defined in Table 70.

Table 70: Categories of MIB-II objects

Objects in category…	Control or identify the status of…
system	system operations in the module.
interfaces	the network interfaces for which the module is configured.
ip	Internet Protocol information in the module.
icmp	Internet Control Message Protocol information in the module. (These messages flag IP problems and allow IP links to be tested.)
tcp	Transport Control Protocol information in the module (to control and ensure the flow of data on the Internet).
udp	User Datagram Protocol information in the module (for checksum and address).

Canopy Enterprise MIB

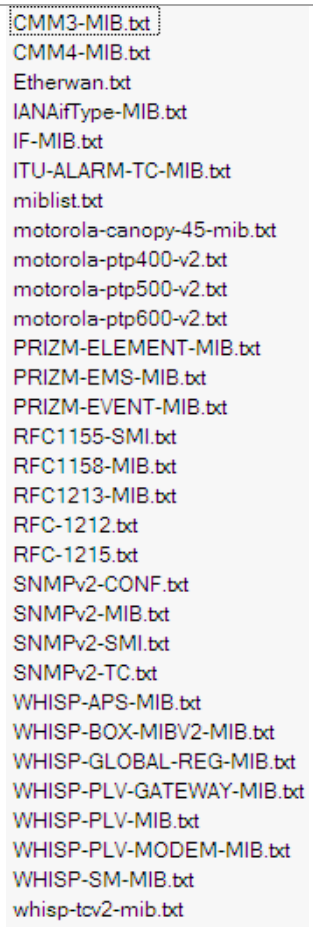
The Canopy Enterprise MIB provides additional reporting and control, extending the objects for any NMS that uses SNMP interaction. This MIB comprises five text files that are formatted in standard ASN.1 (Abstract Syntax Notation One) language.

The installation tool for Prizm places this MIB into the `C:\...\PrizmInstallationDirectory\modules\mibs` directory. The Prizm server software expects to find its contents there.

To use this MIB with an NMS, perform the following steps.

Procedure 36: Installing the Canopy Enterprise MIB files

1. On the NMS, immediately beneath the `root` directory, create directory *`mibviewer`*.
2. Immediately beneath the *`mibviewer`* directory, create directory *`canopymibs`*.
3. Download the following three standard MIB files from the Internet Engineering Task Force at http://www.simpleweb.org/ietf/mibs into the *`mibviewer/canopymibs`* directory on the NMS:
   - SNMPv2-SMI.txt, which defines the Structure of Management Information specifications.
   - SNMPv2-CONF.txt, which allows macros to be defined for object group, notification group, module compliance, and agent capabilities.
   - SNMPv2-TC.txt, which defines general textual conventions.
4. Move the following files or the subset of these files from your software release package directory into the *`mibviewer/canopymibs`* directory on the NMS (if necessary, first download the software package from http://www.cambiumnetworks.com/support/pmp/software/index.php)



IMPORTANT!
Do not edit these MIB files in ASN.1. These files are intended for manipulation by only the NMS. However, you can view these files through a commercially available MIB viewer. Such viewers are listed under MIB Viewers on Page 497.

5. Download a selected MIB viewer into directory *mibviewer*.
6. As instructed by the user documentation that supports your NMS, import the eight MIB files that are listed above.

Configuring Modules for SNMP Access

Canopy modules provide the following Configuration web page parameters in the SNMP tab. These govern SNMP access from the manager to the agent:

- **Community String**, which specifies the password for security between managers and the agent.

- **Accessing Subnet**, which specifies the subnet mask that allows managers to poll the agents.

Canopy modules can also be configured to send traps to specified IP addresses, which can be those of Prizm or NMS servers, for example. The parameter for this address is named **Trap Address**.

Objects Defined in the Canopy Enterprise MIB

The Canopy Enterprise MIB defines separate sets of objects for

- all radio modules (objects common to all devices)
- APs and BH timing masters
- SMs and BH timing slaves
- CMMmicros
- CMM4s

NOTE:
The PTP 300, 400, 500, and 600 series wireless Ethernet bridges do not support these objects.

AP, SM, and BH Objects

The objects that the Canopy Enterprise MIB defines for all APs, SMs, and BHs are listed in Table 71.

Table 71: Canopy Enterprise MIB objects for APs, SMs, and BHs

Name	OID	valueType
whispBoxSoftwareVer.0	.1.3.6.1.4.1.161.19.3.3.1.1.0	OctetString
whispBoxFPGAVer.0	.1.3.6.1.4.1.161.19.3.3.1.2.0	OctetString
whispBoxEsn.0	.1.3.6.1.4.1.161.19.3.3.1.3.0	OctetString
whispBoxBoot.0	.1.3.6.1.4.1.161.19.3.3.1.4.0	OctetString
boxDeviceType.0	.1.3.6.1.4.1.161.19.3.3.1.6.0	OctetString
boxDeviceTypeID.0	.1.3.6.1.4.1.161.19.3.3.1.7.0	OctetString
boxEncryption.0	.1.3.6.1.4.1.161.19.3.3.1.8.0	OctetString

etherLinkStatus.0	.1.3.6.1.4.1.161.19.3.3.1.9.0	OctetString
boxFrequency.0	.1.3.6.1.4.1.161.19.3.3.1.10.0	OctetString
platformVer.0	.1.3.6.1.4.1.161.19.3.3.1.11.0	Integer
platformType.0	.1.3.6.1.4.1.161.19.3.3.1.12.0	OctetString
dhcpLanIp.0	.1.3.6.1.4.1.161.19.3.3.1.13.0	IpAddress
dhcpLanSubnetMask.0	.1.3.6.1.4.1.161.19.3.3.1.14.0	IpAddress
dhcpLanGateway.0	.1.3.6.1.4.1.161.19.3.3.1.15.0	IpAddress
dhcpRfPublicIp.0	.1.3.6.1.4.1.161.19.3.3.1.16.0	IpAddress
dhcpRfPublicSubnetMask.0	.1.3.6.1.4.1.161.19.3.3.1.17.0	IpAddress
dhcpRfPublicGateway.0	.1.3.6.1.4.1.161.19.3.3.1.18.0	IpAddress
lanDhcpStatus.0	.1.3.6.1.4.1.161.19.3.3.1.19.0	OctetString
rfPublicDhcpStatus.0	.1.3.6.1.4.1.161.19.3.3.1.20.0	OctetString
inSyncCount.0	.1.3.6.1.4.1.161.19.3.3.1.21.0	Integer
outSyncCount.0	.1.3.6.1.4.1.161.19.3.3.1.22.0	Integer
pllOutLockCount.0	.1.3.6.1.4.1.161.19.3.3.1.23.0	Integer
txCalFailure.0	.1.3.6.1.4.1.161.19.3.3.1.24.0	Integer
swVersion.0	.1.3.6.1.4.1.161.19.3.3.1.25.0	OctetString
pldVersion.0	.1.3.6.1.4.1.161.19.3.3.1.26.0	OctetString
platformInfo.0	.1.3.6.1.4.1.161.19.3.3.1.27.0	OctetString
antPolarization.0	.1.3.6.1.4.1.161.19.3.3.1.28.0	OctetString
packetOverloadCounter.0	.1.3.6.1.4.1.161.19.3.3.1.29.0	Counter32
whispBoxP11Personality.0	.1.3.6.1.4.1.161.19.3.3.1.30.0	OctetString
whispBoxP11FPGAType.0	.1.3.6.1.4.1.161.19.3.3.1.31.0	OctetString
whispBoxP11BstrapFPGAVer.0	.1.3.6.1.4.1.161.19.3.3.1.32.0	OctetString
rxOverrunPkts.0	.1.3.6.1.4.1.161.19.3.3.1.34.0	Counter32
boxTemperatureC.0	.1.3.6.1.4.1.161.19.3.3.1.35.0	Integer
boxTemperatureF.0	.1.3.6.1.4.1.161.19.3.3.1.36.0	Integer
bridgeCbFecStatbin.0	.1.3.6.1.4.1.161.19.3.3.1.37.0	Counter32
bridgeCbFecStatbout.0	.1.3.6.1.4.1.161.19.3.3.1.38.0	Counter32

bridgeCbFecStatbtoss.0	.1.3.6.1.4.1.161.19.3.3.1.39.0	Counter32
bridgeCbFecStatbtosscap.0	.1.3.6.1.4.1.161.19.3.3.1.40.0	Counter32
bridgeCbFecStatuin.0	.1.3.6.1.4.1.161.19.3.3.1.41.0	Counter32
bridgeCbFecStatuout.0	.1.3.6.1.4.1.161.19.3.3.1.42.0	Counter32
bridgeCbFecStatutoss.0	.1.3.6.1.4.1.161.19.3.3.1.43.0	Counter32
bridgeCbFecStatutosscap.0	.1.3.6.1.4.1.161.19.3.3.1.44.0	Counter32
bridgeCbRFStatbin.0	.1.3.6.1.4.1.161.19.3.3.1.45.0	Counter32
bridgeCbRFStatbout.0	.1.3.6.1.4.1.161.19.3.3.1.46.0	Counter32
bridgeCbRFStatbtoss.0	.1.3.6.1.4.1.161.19.3.3.1.47.0	Counter32
bridgeCbRFStatbtosscap.0	.1.3.6.1.4.1.161.19.3.3.1.48.0	Counter32
bridgeCbRFStatuin.0	.1.3.6.1.4.1.161.19.3.3.1.49.0	Counter32
bridgeCbRFStatuout.0	.1.3.6.1.4.1.161.19.3.3.1.50.0	Counter32
bridgeCbRFStatutoss.0	.1.3.6.1.4.1.161.19.3.3.1.51.0	Counter32
bridgeCbRFStatutosscap.0	.1.3.6.1.4.1.161.19.3.3.1.52.0	Counter32
bridgeCbErrStatNI1QSend.0	.1.3.6.1.4.1.161.19.3.3.1.53.0	Counter32
bridgeCbErrStatNI2QSend.0	.1.3.6.1.4.1.161.19.3.3.1.54.0	Counter32
bridgeCbErrStatBridgeFull.0	.1.3.6.1.4.1.161.19.3.3.1.55.0	Counter32
bridgeCbErrStatSendMsg.0	.1.3.6.1.4.1.161.19.3.3.1.56.0	Counter32
bridgeCbErrStatAPFecQSend.0	.1.3.6.1.4.1.161.19.3.3.1.57.0	Counter32
bridgeCbErrStatApRfQSend.0	.1.3.6.1.4.1.161.19.3.3.1.58.0	Counter32
rfStatXmtUDataCnt.0	.1.3.6.1.4.1.161.19.3.3.1.59.0	Counter32
rfStatXmtBDataCnt.0	.1.3.6.1.4.1.161.19.3.3.1.60.0	Counter32
rfStatRcvUDataCnt.0	.1.3.6.1.4.1.161.19.3.3.1.61.0	Counter32
rfStatRcvBDataCnt.0	.1.3.6.1.4.1.161.19.3.3.1.62.0	Counter32
rfStatXmtCntlCnt.0	.1.3.6.1.4.1.161.19.3.3.1.63.0	Counter32
rfStatRcvCntlCnt.0	.1.3.6.1.4.1.161.19.3.3.1.64.0	Counter32
rfStatInSyncCount.0	.1.3.6.1.4.1.161.19.3.3.1.65.0	Counter32
rfStatOutSyncCount.0	.1.3.6.1.4.1.161.19.3.3.1.66.0	Counter32
rfStatOverrunCount.0	.1.3.6.1.4.1.161.19.3.3.1.67.0	Counter32

rfStatUnderrunCount.0	.1.3.6.1.4.1.161.19.3.3.1.68.0	Counter32
rfStatRcvCorruptDataCount.0	.1.3.6.1.4.1.161.19.3.3.1.69.0	Counter32
rfStatBadBcastCtlCnt.0	.1.3.6.1.4.1.161.19.3.3.1.70.0	Counter32
rfStatPLLOutOfLockCnt.0	.1.3.6.1.4.1.161.19.3.3.1.71.0	Counter32
rfStatBeaconVerMismatchCnt.0	.1.3.6.1.4.1.161.19.3.3.1.72.0	Counter32
rfStatBadFreqBcnRcvCnt.0	.1.3.6.1.4.1.161.19.3.3.1.73.0	Counter32
rfStatnonLiteBcnRcvCnt.0	.1.3.6.1.4.1.161.19.3.3.1.74.0	Counter32
rfStatUnsupFeatBcnRcvCnt.0	.1.3.6.1.4.1.161.19.3.3.1.75.0	Counter32
rfStatUnkwnFeatBcnRcvCnt.0	.1.3.6.1.4.1.161.19.3.3.1.76.0	Counter32
rfStatTxCalFailCnt.0	.1.3.6.1.4.1.161.19.3.3.1.77.0	Counter32
rfStatBadInSyncIDRcv.0	.1.3.6.1.4.1.161.19.3.3.1.78.0	Counter32
rfStatTempOutOfRange.0	.1.3.6.1.4.1.161.19.3.3.1.79.0	Counter32
rfStatRSSIOutOfRange.0	.1.3.6.1.4.1.161.19.3.3.1.80.0	Counter32
rfStatRangeCapEnf.0	.1.3.6.1.4.1.161.19.3.3.1.81.0	Counter32
rfStatRcvLTStart.0	.1.3.6.1.4.1.161.19.3.3.1.82.0	Counter32
rfStatRcvLTStartHS.0	.1.3.6.1.4.1.161.19.3.3.1.83.0	Counter32
rfStatRcvLTResult.0	.1.3.6.1.4.1.161.19.3.3.1.84.0	Counter32
rfStatXmtLTResult.0	.1.3.6.1.4.1.161.19.3.3.1.85.0	Counter32
whispFeatureKeyOrigin.0	.1.3.6.1.4.1.161.19.3.3.1.86.0	OctetString
radioMSN.0	.1.3.6.1.4.1.161.19.3.3.1.87.0	OctetString
colorCode.0	.1.3.6.1.4.1.161.19.3.3.2.2.0	Integer
fullAccess.0	.1.3.6.1.4.1.161.19.3.3.2.4.0	OctetString
webAutoUpdate.0	.1.3.6.1.4.1.161.19.3.3.2.5.0	Integer
pass1Status.0	.1.3.6.1.4.1.161.19.3.3.2.6.0	OctetString
pass2Status.0	.1.3.6.1.4.1.161.19.3.3.2.7.0	OctetString
bridgeEntryTimeout.0	.1.3.6.1.4.1.161.19.3.3.2.8.0	Integer
snmpMibPerm.0	.1.3.6.1.4.1.161.19.3.3.2.9.0	Integer
dynamicLearning.0	.1.3.6.1.4.1.161.19.3.3.2.16.0	Integer
managementVID.0	.1.3.6.1.4.1.161.19.3.3.2.17.0	Integer
agingTimeout.0	.1.3.6.1.4.1.161.19.3.3.2.18.0	Integer

frameType.0	.1.3.6.1.4.1.161.19.3.3.2.19.0	Integer
addVlanMember.0	.1.3.6.1.4.1.161.19.3.3.2.20.0	Integer
removeVlanMember.0	.1.3.6.1.4.1.161.19.3.3.2.21.0	Integer
scheduling.0	.1.3.6.1.4.1.161.19.3.3.2.22.0	Integer
transmitterOP.0	.1.3.6.1.4.1.161.19.3.3.2.23.0	Integer
trapIP1.0	.1.3.6.1.4.1.161.19.3.3.2.26.0	IpAddress
trapIP2.0	.1.3.6.1.4.1.161.19.3.3.2.27.0	IpAddress
trapIP3.0	.1.3.6.1.4.1.161.19.3.3.2.28.0	IpAddress
trapIP4.0	.1.3.6.1.4.1.161.19.3.3.2.29.0	IpAddress
trapIP5.0	.1.3.6.1.4.1.161.19.3.3.2.30.0	IpAddress
trapIP6.0	.1.3.6.1.4.1.161.19.3.3.2.31.0	IpAddress
trapIP7.0	.1.3.6.1.4.1.161.19.3.3.2.32.0	IpAddress
trapIP8.0	.1.3.6.1.4.1.161.19.3.3.2.33.0	IpAddress
trapIP9.0	.1.3.6.1.4.1.161.19.3.3.2.34.0	IpAddress
trapIP10.0	.1.3.6.1.4.1.161.19.3.3.2.35.0	IpAddress
commStringRWrite.0	.1.3.6.1.4.1.161.19.3.3.2.36.0	OctetString
subnetMask.0	.1.3.6.1.4.1.161.19.3.3.2.37.0	Integer
mngtIP.0	.1.3.6.1.4.1.161.19.3.3.2.38.0	IpAddress
allowVIDAccess.0	.1.3.6.1.4.1.161.19.3.3.2.39.0	Integer
setDefaultPlug.0	.1.3.6.1.4.1.161.19.3.3.2.40.0	Integer
gpsInput.0	.1.3.6.1.4.1.161.19.3.3.2.42.0	Integer
userName.0	.1.3.6.1.4.1.161.19.3.3.2.45.0	OctetString
userPassword.0	.1.3.6.1.4.1.161.19.3.3.2.46.0	OctetString
userAccessLevel.0	.1.3.6.1.4.1.161.19.3.3.2.47.0	Integer
deleteUser.0	.1.3.6.1.4.1.161.19.3.3.2.48.0	OctetString
lanDhcpState.0	.1.3.6.1.4.1.161.19.3.3.2.50.0	Integer
sessionTimeout.0	.1.3.6.1.4.1.161.19.3.3.2.51.0	Integer
vlanMemberSource.0	.1.3.6.1.4.1.161.19.3.3.2.52.0	Integer
changeUsrPwd.0	.1.3.6.1.4.1.161.19.3.3.2.56.0	OctetString

mngtIP2.0	.1.3.6.1.4.1.161.19.3.3.2.57.0	IpAddress
subnetMask2.0	.1.3.6.1.4.1.161.19.3.3.2.58.0	Integer
mngtIP3.0	.1.3.6.1.4.1.161.19.3.3.2.59.0	IpAddress
subnetMask3.0	.1.3.6.1.4.1.161.19.3.3.2.60.0	Integer
mngtIP4.0	.1.3.6.1.4.1.161.19.3.3.2.61.0	IpAddress
subnetMask4.0	.1.3.6.1.4.1.161.19.3.3.2.62.0	Integer
mngtIP5.0	.1.3.6.1.4.1.161.19.3.3.2.63.0	IpAddress
subnetMask5.0	.1.3.6.1.4.1.161.19.3.3.2.64.0	Integer
mngtIP6.0	.1.3.6.1.4.1.161.19.3.3.2.65.0	IpAddress
subnetMask6.0	.1.3.6.1.4.1.161.19.3.3.2.66.0	Integer
mngtIP7.0	.1.3.6.1.4.1.161.19.3.3.2.67.0	IpAddress
subnetMask7.0	.1.3.6.1.4.1.161.19.3.3.2.68.0	Integer
mngtIP8.0	.1.3.6.1.4.1.161.19.3.3.2.69.0	IpAddress
subnetMask8.0	.1.3.6.1.4.1.161.19.3.3.2.70.0	Integer
mngtIP9.0	.1.3.6.1.4.1.161.19.3.3.2.71.0	IpAddress
subnetMask9.0	.1.3.6.1.4.1.161.19.3.3.2.72.0	Integer
mngtIP10.0	.1.3.6.1.4.1.161.19.3.3.2.73.0	IpAddress
subnetMask10.0	.1.3.6.1.4.1.161.19.3.3.2.74.0	Integer
lldpBroadcastEnable.0	.1.3.6.1.4.1.161.19.3.3.2.76.0	Integer
regionCode.0	.1.3.6.1.4.1.161.19.3.3.2.77.0	Integer
commStringROnly.0	.1.3.6.1.4.1.161.19.3.3.2.79.0	OctetString
ethernetLinkSpeed.0	.1.3.6.1.4.1.161.19.3.3.2.80.0	Integer
setDefaults.0	.1.3.6.1.4.1.161.19.3.3.2.84.0	Integer
radioRateAdapt.0	.1.3.6.1.4.1.161.19.3.3.2.85.0	Integer
siteInfoViewable.0	.1.3.6.1.4.1.161.19.3.3.2.86.0	Integer
latitude.0	.1.3.6.1.4.1.161.19.3.3.2.88.0	OctetString
longitude.0	.1.3.6.1.4.1.161.19.3.3.2.89.0	OctetString
height.0	.1.3.6.1.4.1.161.19.3.3.2.90.0	Integer
bandwidth.0	.1.3.6.1.4.1.161.19.3.3.2.91.0	Integer
whispWebUserAccessMode.0	.1.3.6.1.4.1.161.19.3.3.2.118.0	Integer

usrAccountEnableAccounting.0	.1.3.6.1.4.1.161.19.3.3.2.119.0	Integer
allowRejectThenLocal.0	.1.3.6.1.4.1.161.19.3.3.2.120.0	Integer
snrCalculation.0	.1.3.6.1.4.1.161.19.3.3.2.121.0	Integer
priorityPrecedence.0	.1.3.6.1.4.1.161.19.3.3.2.122.0	Integer
installationColorCode.0	.1.3.6.1.4.1.161.19.3.3.2.123.0	Integer
apSmMode.0	.1.3.6.1.4.1.161.19.3.3.2.124.0	Integer
pppoeFilter.0	.1.3.6.1.4.1.161.19.3.3.2.125.0	Integer
smbFilter.0	.1.3.6.1.4.1.161.19.3.3.2.126.0	Integer
snmpFilter.0	.1.3.6.1.4.1.161.19.3.3.2.127.0	Integer
userP1Filter.0	.1.3.6.1.4.1.161.19.3.3.2.128.0	Integer
userP2Filter.0	.1.3.6.1.4.1.161.19.3.3.2.129.0	Integer
userP3Filter.0	.1.3.6.1.4.1.161.19.3.3.2.130.0	Integer
allOtherIpFilter.0	.1.3.6.1.4.1.161.19.3.3.2.131.0	Integer
allIpv4Filter.0	.1.3.6.1.4.1.161.19.3.3.2.132.0	Integer
arpFilter.0	.1.3.6.1.4.1.161.19.3.3.2.133.0	Integer
allOthersFilter.0	.1.3.6.1.4.1.161.19.3.3.2.134.0	Integer
userDefinedPort1.0	.1.3.6.1.4.1.161.19.3.3.2.135.0	Integer
port1TCPFilter.0	.1.3.6.1.4.1.161.19.3.3.2.136.0	Integer
port1UDPFilter.0	.1.3.6.1.4.1.161.19.3.3.2.137.0	Integer
userDefinedPort2.0	.1.3.6.1.4.1.161.19.3.3.2.138.0	Integer
port2TCPFilter.0	.1.3.6.1.4.1.161.19.3.3.2.139.0	Integer
port2UDPFilter.0	.1.3.6.1.4.1.161.19.3.3.2.140.0	Integer
userDefinedPort3.0	.1.3.6.1.4.1.161.19.3.3.2.141.0	Integer
port3TCPFilter.0	.1.3.6.1.4.1.161.19.3.3.2.142.0	Integer
port3UDPFilter.0	.1.3.6.1.4.1.161.19.3.3.2.143.0	Integer
bootpcFilter.0	.1.3.6.1.4.1.161.19.3.3.2.144.0	Integer
bootpsFilter.0	.1.3.6.1.4.1.161.19.3.3.2.145.0	Integer
ip4MultFilter.0	.1.3.6.1.4.1.161.19.3.3.2.146.0	Integer
packetFilterDirection.0	.1.3.6.1.4.1.161.19.3.3.2.147.0	Integer

pppoeCtlPriority.0	.1.3.6.1.4.1.161.19.3.3.2.149.0	Integer
reboot.0	.1.3.6.1.4.1.161.19.3.3.3.2.0	Integer
clearEventLog.0	.1.3.6.1.4.1.161.19.3.3.3.3.0	Integer
rebootIfRequired.0	.1.3.6.1.4.1.161.19.3.3.3.4.0	Integer
clearBERStats.0	.1.3.6.1.4.1.161.19.3.3.3.5.0	Integer
whispBridgeMacAddr.1	.1.3.6.1.4.1.161.19.3.3.4.1.1.1	OctetString
whispBridgeMacAddr.2	.1.3.6.1.4.1.161.19.3.3.4.1.1.2	OctetString
whispBridgeMacAddr.3	.1.3.6.1.4.1.161.19.3.3.4.1.1.3	OctetString
whispBridgeMacAddr.4	.1.3.6.1.4.1.161.19.3.3.4.1.1.4	OctetString
whispBridgeMacAddr.5	.1.3.6.1.4.1.161.19.3.3.4.1.1.5	OctetString
whispBridgeDesLuid.1	.1.3.6.1.4.1.161.19.3.3.4.1.2.1	Integer
whispBridgeDesLuid.2	.1.3.6.1.4.1.161.19.3.3.4.1.2.2	Integer
whispBridgeDesLuid.3	.1.3.6.1.4.1.161.19.3.3.4.1.2.3	Integer
whispBridgeDesLuid.4	.1.3.6.1.4.1.161.19.3.3.4.1.2.4	Integer
whispBridgeDesLuid.5	.1.3.6.1.4.1.161.19.3.3.4.1.2.5	Integer
whispBridgeAge.1	.1.3.6.1.4.1.161.19.3.3.4.1.3.1	Integer
whispBridgeAge.2	.1.3.6.1.4.1.161.19.3.3.4.1.3.2	Integer
whispBridgeAge.3	.1.3.6.1.4.1.161.19.3.3.4.1.3.3	Integer
whispBridgeAge.4	.1.3.6.1.4.1.161.19.3.3.4.1.3.4	Integer
whispBridgeAge.5	.1.3.6.1.4.1.161.19.3.3.4.1.3.5	Integer
whispBridgeExt.1	.1.3.6.1.4.1.161.19.3.3.4.1.4.1	Integer
whispBridgeExt.2	.1.3.6.1.4.1.161.19.3.3.4.1.4.2	Integer
whispBridgeExt.3	.1.3.6.1.4.1.161.19.3.3.4.1.4.3	Integer
whispBridgeExt.4	.1.3.6.1.4.1.161.19.3.3.4.1.4.4	Integer
whispBridgeExt.5	.1.3.6.1.4.1.161.19.3.3.4.1.4.5	Integer
whispBridgeHash.1	.1.3.6.1.4.1.161.19.3.3.4.1.5.1	Integer
whispBridgeHash.2	.1.3.6.1.4.1.161.19.3.3.4.1.5.2	Integer
whispBridgeHash.3	.1.3.6.1.4.1.161.19.3.3.4.1.5.3	Integer
whispBridgeHash.4	.1.3.6.1.4.1.161.19.3.3.4.1.5.4	Integer
whispBridgeHash.5	.1.3.6.1.4.1.161.19.3.3.4.1.5.5	Integer

whispBoxEvntLog.0	.1.3.6.1.4.1.161.19.3.3.5.1.0	OctetString
whispBridgeTbUsed.0	.1.3.6.1.4.1.161.19.3.3.7.1.0	Integer
whispBridgeTbFree.0	.1.3.6.1.4.1.161.19.3.3.7.2.0	Integer
whispBridgeTbErr.0	.1.3.6.1.4.1.161.19.3.3.7.3.0	Integer
whispVID.1	.1.3.6.1.4.1.161.19.3.3.8.1.1.1	Integer
whispVID.2	.1.3.6.1.4.1.161.19.3.3.8.1.1.2	Integer
whispVType.1	.1.3.6.1.4.1.161.19.3.3.8.1.2.1	OctetString
whispVType.2	.1.3.6.1.4.1.161.19.3.3.8.1.2.2	OctetString
whispVAge.1	.1.3.6.1.4.1.161.19.3.3.8.1.3.1	Integer
whispVAge.2	.1.3.6.1.4.1.161.19.3.3.8.1.3.2	Integer
codePoint0.0	.1.3.6.1.4.1.161.19.3.3.9.1.0	Integer
codePoint1.0	.1.3.6.1.4.1.161.19.3.3.9.2.0	Integer
codePoint2.0	.1.3.6.1.4.1.161.19.3.3.9.3.0	Integer
codePoint3.0	.1.3.6.1.4.1.161.19.3.3.9.4.0	Integer
codePoint4.0	.1.3.6.1.4.1.161.19.3.3.9.5.0	Integer
codePoint5.0	.1.3.6.1.4.1.161.19.3.3.9.6.0	Integer
codePoint6.0	.1.3.6.1.4.1.161.19.3.3.9.7.0	Integer
codePoint7.0	.1.3.6.1.4.1.161.19.3.3.9.8.0	Integer
codePoint8.0	.1.3.6.1.4.1.161.19.3.3.9.9.0	Integer
codePoint9.0	.1.3.6.1.4.1.161.19.3.3.9.10.0	Integer
codePoint10.0	.1.3.6.1.4.1.161.19.3.3.9.11.0	Integer
codePoint11.0	.1.3.6.1.4.1.161.19.3.3.9.12.0	Integer
codePoint12.0	.1.3.6.1.4.1.161.19.3.3.9.13.0	Integer
codePoint13.0	.1.3.6.1.4.1.161.19.3.3.9.14.0	Integer
codePoint14.0	.1.3.6.1.4.1.161.19.3.3.9.15.0	Integer
codePoint15.0	.1.3.6.1.4.1.161.19.3.3.9.16.0	Integer
codePoint16.0	.1.3.6.1.4.1.161.19.3.3.9.17.0	Integer
codePoint17.0	.1.3.6.1.4.1.161.19.3.3.9.18.0	Integer
codePoint18.0	.1.3.6.1.4.1.161.19.3.3.9.19.0	Integer

codePoint19.0	.1.3.6.1.4.1.161.19.3.3.9.20.0	Integer
codePoint20.0	.1.3.6.1.4.1.161.19.3.3.9.21.0	Integer
codePoint21.0	.1.3.6.1.4.1.161.19.3.3.9.22.0	Integer
codePoint22.0	.1.3.6.1.4.1.161.19.3.3.9.23.0	Integer
codePoint23.0	.1.3.6.1.4.1.161.19.3.3.9.24.0	Integer
codePoint24.0	.1.3.6.1.4.1.161.19.3.3.9.25.0	Integer
codePoint25.0	.1.3.6.1.4.1.161.19.3.3.9.26.0	Integer
codePoint26.0	.1.3.6.1.4.1.161.19.3.3.9.27.0	Integer
codePoint27.0	.1.3.6.1.4.1.161.19.3.3.9.28.0	Integer
codePoint28.0	.1.3.6.1.4.1.161.19.3.3.9.29.0	Integer
codePoint29.0	.1.3.6.1.4.1.161.19.3.3.9.30.0	Integer
codePoint30.0	.1.3.6.1.4.1.161.19.3.3.9.31.0	Integer
codePoint31.0	.1.3.6.1.4.1.161.19.3.3.9.32.0	Integer
codePoint32.0	.1.3.6.1.4.1.161.19.3.3.9.33.0	Integer
codePoint33.0	.1.3.6.1.4.1.161.19.3.3.9.34.0	Integer
codePoint34.0	.1.3.6.1.4.1.161.19.3.3.9.35.0	Integer
codePoint35.0	.1.3.6.1.4.1.161.19.3.3.9.36.0	Integer
codePoint36.0	.1.3.6.1.4.1.161.19.3.3.9.37.0	Integer
codePoint37.0	.1.3.6.1.4.1.161.19.3.3.9.38.0	Integer
codePoint38.0	.1.3.6.1.4.1.161.19.3.3.9.39.0	Integer
codePoint39.0	.1.3.6.1.4.1.161.19.3.3.9.40.0	Integer
codePoint40.0	.1.3.6.1.4.1.161.19.3.3.9.41.0	Integer
codePoint41.0	.1.3.6.1.4.1.161.19.3.3.9.42.0	Integer
codePoint42.0	.1.3.6.1.4.1.161.19.3.3.9.43.0	Integer
codePoint43.0	.1.3.6.1.4.1.161.19.3.3.9.44.0	Integer
codePoint44.0	.1.3.6.1.4.1.161.19.3.3.9.45.0	Integer
codePoint45.0	.1.3.6.1.4.1.161.19.3.3.9.46.0	Integer
codePoint46.0	.1.3.6.1.4.1.161.19.3.3.9.47.0	Integer
codePoint47.0	.1.3.6.1.4.1.161.19.3.3.9.48.0	Integer
codePoint48.0	.1.3.6.1.4.1.161.19.3.3.9.49.0	Integer

codePoint49.0	.1.3.6.1.4.1.161.19.3.3.9.50.0	Integer
codePoint50.0	.1.3.6.1.4.1.161.19.3.3.9.51.0	Integer
codePoint51.0	.1.3.6.1.4.1.161.19.3.3.9.52.0	Integer
codePoint52.0	.1.3.6.1.4.1.161.19.3.3.9.53.0	Integer
codePoint53.0	.1.3.6.1.4.1.161.19.3.3.9.54.0	Integer
codePoint54.0	.1.3.6.1.4.1.161.19.3.3.9.55.0	Integer
codePoint55.0	.1.3.6.1.4.1.161.19.3.3.9.56.0	Integer
codePoint56.0	.1.3.6.1.4.1.161.19.3.3.9.57.0	Integer
codePoint57.0	.1.3.6.1.4.1.161.19.3.3.9.58.0	Integer
codePoint58.0	.1.3.6.1.4.1.161.19.3.3.9.59.0	Integer
codePoint59.0	.1.3.6.1.4.1.161.19.3.3.9.60.0	Integer
codePoint60.0	.1.3.6.1.4.1.161.19.3.3.9.61.0	Integer
codePoint61.0	.1.3.6.1.4.1.161.19.3.3.9.62.0	Integer
codePoint62.0	.1.3.6.1.4.1.161.19.3.3.9.63.0	Integer
codePoint63.0	.1.3.6.1.4.1.161.19.3.3.9.64.0	Integer
entryIndex.1	.1.3.6.1.4.1.161.19.3.3.10.1.1.1	Integer
entryIndex.2	.1.3.6.1.4.1.161.19.3.3.10.1.1.2	Integer
entryIndex.3	.1.3.6.1.4.1.161.19.3.3.10.1.1.3	Integer
entryIndex.4	.1.3.6.1.4.1.161.19.3.3.10.1.1.4	Integer
userLoginName.1	.1.3.6.1.4.1.161.19.3.3.10.1.2.1	OctetString
userLoginName.2	.1.3.6.1.4.1.161.19.3.3.10.1.2.2	OctetString
userLoginName.3	.1.3.6.1.4.1.161.19.3.3.10.1.2.3	OctetString
userLoginName.4	.1.3.6.1.4.1.161.19.3.3.10.1.2.4	OctetString
userPswd.1	.1.3.6.1.4.1.161.19.3.3.10.1.3.1	OctetString
userPswd.2	.1.3.6.1.4.1.161.19.3.3.10.1.3.2	OctetString
userPswd.3	.1.3.6.1.4.1.161.19.3.3.10.1.3.3	OctetString
userPswd.4	.1.3.6.1.4.1.161.19.3.3.10.1.3.4	OctetString
accessLevel.1	.1.3.6.1.4.1.161.19.3.3.10.1.4.1	Integer
accessLevel.2	.1.3.6.1.4.1.161.19.3.3.10.1.4.2	Integer

accessLevel.3	.1.3.6.1.4.1.161.19.3.3.10.1.4.3	Integer
accessLevel.4	.1.3.6.1.4.1.161.19.3.3.10.1.4.4	Integer
loginStatus.1	.1.3.6.1.4.1.161.19.3.3.10.1.5.1	Integer
loginStatus.2	.1.3.6.1.4.1.161.19.3.3.10.1.5.2	Integer
loginStatus.3	.1.3.6.1.4.1.161.19.3.3.10.1.5.3	Integer
loginStatus.4	.1.3.6.1.4.1.161.19.3.3.10.1.5.4	Integer
loginMethod.1	.1.3.6.1.4.1.161.19.3.3.10.1.6.1	Integer
loginMethod.2	.1.3.6.1.4.1.161.19.3.3.10.1.6.2	Integer
loginMethod.3	.1.3.6.1.4.1.161.19.3.3.10.1.6.3	Integer
loginMethod.4	.1.3.6.1.4.1.161.19.3.3.10.1.6.4	Integer
sessionTime.1	.1.3.6.1.4.1.161.19.3.3.10.1.7.1	Integer
sessionTime.2	.1.3.6.1.4.1.161.19.3.3.10.1.7.2	Integer
sessionTime.3	.1.3.6.1.4.1.161.19.3.3.10.1.7.3	Integer
sessionTime.4	.1.3.6.1.4.1.161.19.3.3.10.1.7.4	Integer
neighborMAC.1	.1.3.6.1.4.1.161.19.3.3.11.1.2.1	OctetString
neighborMAC.2	.1.3.6.1.4.1.161.19.3.3.11.1.2.2	OctetString
neighborMAC.3	.1.3.6.1.4.1.161.19.3.3.11.1.2.3	OctetString
neighborMAC.4	.1.3.6.1.4.1.161.19.3.3.11.1.2.4	OctetString
neighborMAC.5	.1.3.6.1.4.1.161.19.3.3.11.1.2.5	OctetString
neighborMAC.6	.1.3.6.1.4.1.161.19.3.3.11.1.2.6	OctetString
neighborMAC.7	.1.3.6.1.4.1.161.19.3.3.11.1.2.7	OctetString
neighborMAC.8	.1.3.6.1.4.1.161.19.3.3.11.1.2.8	OctetString
neighborMAC.9	.1.3.6.1.4.1.161.19.3.3.11.1.2.9	OctetString
neighborMAC.10	.1.3.6.1.4.1.161.19.3.3.11.1.2.10	OctetString
neighborMAC.11	.1.3.6.1.4.1.161.19.3.3.11.1.2.11	OctetString
neighborMAC.12	.1.3.6.1.4.1.161.19.3.3.11.1.2.12	OctetString
neighborMAC.13	.1.3.6.1.4.1.161.19.3.3.11.1.2.13	OctetString
neighborMAC.14	.1.3.6.1.4.1.161.19.3.3.11.1.2.14	OctetString
neighborMAC.15	.1.3.6.1.4.1.161.19.3.3.11.1.2.15	OctetString
neighborMAC.16	.1.3.6.1.4.1.161.19.3.3.11.1.2.16	OctetString

neighborMAC.17	.1.3.6.1.4.1.161.19.3.3.11.1.2.17	OctetString
neighborMAC.18	.1.3.6.1.4.1.161.19.3.3.11.1.2.18	OctetString
neighborMAC.19	.1.3.6.1.4.1.161.19.3.3.11.1.2.19	OctetString
neighborMAC.20	.1.3.6.1.4.1.161.19.3.3.11.1.2.20	OctetString
neighborIP.1	.1.3.6.1.4.1.161.19.3.3.11.1.3.1	OctetString
neighborIP.2	.1.3.6.1.4.1.161.19.3.3.11.1.3.2	OctetString
neighborIP.3	.1.3.6.1.4.1.161.19.3.3.11.1.3.3	OctetString
neighborIP.4	.1.3.6.1.4.1.161.19.3.3.11.1.3.4	OctetString
neighborIP.5	.1.3.6.1.4.1.161.19.3.3.11.1.3.5	OctetString
neighborIP.6	.1.3.6.1.4.1.161.19.3.3.11.1.3.6	OctetString
neighborIP.7	.1.3.6.1.4.1.161.19.3.3.11.1.3.7	OctetString
neighborIP.8	.1.3.6.1.4.1.161.19.3.3.11.1.3.8	OctetString
neighborIP.9	.1.3.6.1.4.1.161.19.3.3.11.1.3.9	OctetString
neighborIP.10	.1.3.6.1.4.1.161.19.3.3.11.1.3.10	OctetString
neighborIP.11	.1.3.6.1.4.1.161.19.3.3.11.1.3.11	OctetString
neighborIP.12	.1.3.6.1.4.1.161.19.3.3.11.1.3.12	OctetString
neighborIP.13	.1.3.6.1.4.1.161.19.3.3.11.1.3.13	OctetString
neighborIP.14	.1.3.6.1.4.1.161.19.3.3.11.1.3.14	OctetString
neighborIP.15	.1.3.6.1.4.1.161.19.3.3.11.1.3.15	OctetString
neighborIP.16	.1.3.6.1.4.1.161.19.3.3.11.1.3.16	OctetString
neighborIP.17	.1.3.6.1.4.1.161.19.3.3.11.1.3.17	OctetString
neighborIP.18	.1.3.6.1.4.1.161.19.3.3.11.1.3.18	OctetString
neighborIP.19	.1.3.6.1.4.1.161.19.3.3.11.1.3.19	OctetString
neighborIP.20	.1.3.6.1.4.1.161.19.3.3.11.1.3.20	OctetString
neighborSiteName.1	.1.3.6.1.4.1.161.19.3.3.11.1.4.1	OctetString
neighborSiteName.2	.1.3.6.1.4.1.161.19.3.3.11.1.4.2	OctetString
neighborSiteName.3	.1.3.6.1.4.1.161.19.3.3.11.1.4.3	OctetString
neighborSiteName.4	.1.3.6.1.4.1.161.19.3.3.11.1.4.4	OctetString
neighborSiteName.5	.1.3.6.1.4.1.161.19.3.3.11.1.4.5	OctetString

neighborSiteName.6	.1.3.6.1.4.1.161.19.3.3.11.1.4.6	OctetString
neighborSiteName.7	.1.3.6.1.4.1.161.19.3.3.11.1.4.7	OctetString
neighborSiteName.8	.1.3.6.1.4.1.161.19.3.3.11.1.4.8	OctetString
neighborSiteName.9	.1.3.6.1.4.1.161.19.3.3.11.1.4.9	OctetString
neighborSiteName.10	.1.3.6.1.4.1.161.19.3.3.11.1.4.10	OctetString
neighborSiteName.11	.1.3.6.1.4.1.161.19.3.3.11.1.4.11	OctetString
neighborSiteName.12	.1.3.6.1.4.1.161.19.3.3.11.1.4.12	OctetString
neighborSiteName.13	.1.3.6.1.4.1.161.19.3.3.11.1.4.13	OctetString
neighborSiteName.14	.1.3.6.1.4.1.161.19.3.3.11.1.4.14	OctetString
neighborSiteName.15	.1.3.6.1.4.1.161.19.3.3.11.1.4.15	OctetString
neighborSiteName.16	.1.3.6.1.4.1.161.19.3.3.11.1.4.16	OctetString
neighborSiteName.17	.1.3.6.1.4.1.161.19.3.3.11.1.4.17	OctetString
neighborSiteName.18	.1.3.6.1.4.1.161.19.3.3.11.1.4.18	OctetString
neighborSiteName.19	.1.3.6.1.4.1.161.19.3.3.11.1.4.19	OctetString
neighborSiteName.20	.1.3.6.1.4.1.161.19.3.3.11.1.4.20	OctetString
dnsIpState.0	.1.3.6.1.4.1.161.19.3.3.13.1.0	Integer
dnsPrimaryMgmtIP.0	.1.3.6.1.4.1.161.19.3.3.13.2.0	IpAddress
dnsAlternateMgmtIP.0	.1.3.6.1.4.1.161.19.3.3.13.3.0	IpAddress
dnsMgmtDomainName.0	.1.3.6.1.4.1.161.19.3.3.13.4.0	OctetString
trapDomainNameAppend.0	.1.3.6.1.4.1.161.19.3.3.13.5.0	Integer
trap1.0	.1.3.6.1.4.1.161.19.3.3.13.6.0	OctetString
trap2.0	.1.3.6.1.4.1.161.19.3.3.13.7.0	OctetString
trap3.0	.1.3.6.1.4.1.161.19.3.3.13.8.0	OctetString
trap4.0	.1.3.6.1.4.1.161.19.3.3.13.9.0	OctetString
trap5.0	.1.3.6.1.4.1.161.19.3.3.13.10.0	OctetString
trap6.0	.1.3.6.1.4.1.161.19.3.3.13.11.0	OctetString
trap7.0	.1.3.6.1.4.1.161.19.3.3.13.12.0	OctetString
trap8.0	.1.3.6.1.4.1.161.19.3.3.13.13.0	OctetString
trap9.0	.1.3.6.1.4.1.161.19.3.3.13.14.0	OctetString
trap10.0	.1.3.6.1.4.1.161.19.3.3.13.15.0	OctetString

AP and BH Timing Master Objects

The objects that the Canopy Enterprise MIB defines for each AP and BH Timing Master are listed in Table 72. The traps provided in this set of objects are listed under Traps Provided in the Canopy Enterprise MIB on Page 497.

Table 72: Canopy Enterprise MIB objects for APs and BH timing masters

Name	OID	valueType
rfFreqCarrier.0	.1.3.6.1.4.1.161.19.3.1.1.2.0	Integer
dwnLnkData.0	.1.3.6.1.4.1.161.19.3.1.1.4.0	Integer
upLnkDataRate.0	.1.3.6.1.4.1.161.19.3.1.1.12.0	Integer
upLnkLimit.0	.1.3.6.1.4.1.161.19.3.1.1.13.0	Integer
dwnLnkDataRate.0	.1.3.6.1.4.1.161.19.3.1.1.14.0	Integer
dwnLnkLimit.0	.1.3.6.1.4.1.161.19.3.1.1.15.0	Integer
sectorID.0	.1.3.6.1.4.1.161.19.3.1.1.16.0	Integer
maxRange.0	.1.3.6.1.4.1.161.19.3.1.1.17.0	Integer
asIP1.0	.1.3.6.1.4.1.161.19.3.1.1.20.0	IpAddress
asIP2.0	.1.3.6.1.4.1.161.19.3.1.1.21.0	IpAddress
asIP3.0	.1.3.6.1.4.1.161.19.3.1.1.22.0	IpAddress
lanIpAp.0	.1.3.6.1.4.1.161.19.3.1.1.23.0	IpAddress
lanMaskAp.0	.1.3.6.1.4.1.161.19.3.1.1.24.0	IpAddress
defaultGwAp.0	.1.3.6.1.4.1.161.19.3.1.1.25.0	IpAddress
privateIp.0	.1.3.6.1.4.1.161.19.3.1.1.26.0	IpAddress
gpsTrap.0	.1.3.6.1.4.1.161.19.3.1.1.27.0	Integer
regTrap.0	.1.3.6.1.4.1.161.19.3.1.1.28.0	Integer
txSpreading.0	.1.3.6.1.4.1.161.19.3.1.1.29.0	Integer
apBeaconInfo.0	.1.3.6.1.4.1.161.19.3.1.1.30.0	Integer
authMode.0	.1.3.6.1.4.1.161.19.3.1.1.31.0	Integer
authKeyAp.0	.1.3.6.1.4.1.161.19.3.1.1.32.0	OctetString
encryptionMode.0	.1.3.6.1.4.1.161.19.3.1.1.33.0	Integer

ntpServerIp.0	.1.3.6.1.4.1.161.19.3.1.1.34.0	IpAddress
broadcastRetryCount.0	.1.3.6.1.4.1.161.19.3.1.1.35.0	Integer
encryptDwBroadcast.0	.1.3.6.1.4.1.161.19.3.1.1.36.0	Integer
updateAppAddress.0	.1.3.6.1.4.1.161.19.3.1.1.37.0	IpAddress
vlanEnable.0	.1.3.6.1.4.1.161.19.3.1.1.39.0	Integer
configSource.0	.1.3.6.1.4.1.161.19.3.1.1.40.0	Integer
numCtlSlotsHW.0	.1.3.6.1.4.1.161.19.3.1.1.42.0	Integer
displayAPEval.0	.1.3.6.1.4.1.161.19.3.1.1.43.0	Integer
smIsolation.0	.1.3.6.1.4.1.161.19.3.1.1.44.0	Integer
ipAccessFilterEnable.0	.1.3.6.1.4.1.161.19.3.1.1.45.0	Integer
allowedIPAccess1.0	.1.3.6.1.4.1.161.19.3.1.1.46.0	IpAddress
allowedIPAccess2.0	.1.3.6.1.4.1.161.19.3.1.1.47.0	IpAddress
allowedIPAccess3.0	.1.3.6.1.4.1.161.19.3.1.1.48.0	IpAddress
tslBridging.0	.1.3.6.1.4.1.161.19.3.1.1.49.0	Integer
untranslatedArp.0	.1.3.6.1.4.1.161.19.3.1.1.50.0	Integer
limitFreqBand900.0	.1.3.6.1.4.1.161.19.3.1.1.51.0	Integer
scheduleWhitening.0	.1.3.6.1.4.1.161.19.3.1.1.55.0	Integer
remoteSpectrumAnalysisDuration.0	.1.3.6.1.4.1.161.19.3.1.1.56.0	Integer
remoteSpectrumAnalyzerLUID.0	.1.3.6.1.4.1.161.19.3.1.1.57.0	Integer
dlnkBcastCIR.0	.1.3.6.1.4.1.161.19.3.1.1.59.0	Integer
verifyGPSChecksum.0	.1.3.6.1.4.1.161.19.3.1.1.60.0	Integer
apVlanOverride.0	.1.3.6.1.4.1.161.19.3.1.1.61.0	Integer
dhcpRelayAgentEnable.0	.1.3.6.1.4.1.161.19.3.1.1.62.0	Integer
dhcpRelayAgentSrvrIP.0	.1.3.6.1.4.1.161.19.3.1.1.63.0	IpAddress
colorCodeRescanTimer.0	.1.3.6.1.4.1.161.19.3.1.1.64.0	Integer
colorCodeRescanIdleTimer.0	.1.3.6.1.4.1.161.19.3.1.1.65.0	Integer
authKeyOptionAP.0	.1.3.6.1.4.1.161.19.3.1.1.66.0	Integer
asIP4.0	.1.3.6.1.4.1.161.19.3.1.1.67.0	IpAddress
asIP5.0	.1.3.6.1.4.1.161.19.3.1.1.68.0	IpAddress
onlyAllowVer95OrAbove.0	.1.3.6.1.4.1.161.19.3.1.1.69.0	Integer

apRxDelay.0	.1.3.6.1.4.1.161.19.3.1.1.70.0	Integer
qinqEthType.0	.1.3.6.1.4.1.161.19.3.1.1.71.0	Integer
fskSMTxPwrCntl.0	.1.3.6.1.4.1.161.19.3.1.1.72.0	Integer
fskSMRcvTargetLvl.0	.1.3.6.1.4.1.161.19.3.1.1.73.0	Integer
authSharedSecret1.0	.1.3.6.1.4.1.161.19.3.1.1.74.0	OctetString
authSharedSecret2.0	.1.3.6.1.4.1.161.19.3.1.1.75.0	OctetString
authSharedSecret3.0	.1.3.6.1.4.1.161.19.3.1.1.76.0	OctetString
whispUsrAuthSharedSecret1.0	.1.3.6.1.4.1.161.19.3.1.1.79.0	OctetString
whispUsrAuthSharedSecret2.0	.1.3.6.1.4.1.161.19.3.1.1.80.0	OctetString
whispUsrAuthSharedSecret3.0	.1.3.6.1.4.1.161.19.3.1.1.81.0	OctetString
whispUsrAcctSvr1.0	.1.3.6.1.4.1.161.19.3.1.1.82.0	OctetString
whispUsrAcctSvr2.0	.1.3.6.1.4.1.161.19.3.1.1.83.0	OctetString
whispUsrAcctSvr3.0	.1.3.6.1.4.1.161.19.3.1.1.84.0	OctetString
whispUsrAuthPhase1.0	.1.3.6.1.4.1.161.19.3.1.1.85.0	Integer
whispWebUseAuthServer.0	.1.3.6.1.4.1.161.19.3.1.1.86.0	Integer
dropSession.0	.1.3.6.1.4.1.161.19.3.1.1.87.0	OctetString
timeZone.0	.1.3.6.1.4.1.161.19.3.1.1.89.0	Integer
radiusPort.0	.1.3.6.1.4.1.161.19.3.1.1.91.0	Integer
radiusAcctPort.0	.1.3.6.1.4.1.161.19.3.1.1.92.0	Integer
lastSesStatsReset.0	.1.3.6.1.4.1.161.19.3.1.1.93.0	OctetString
resetSesStats.0	.1.3.6.1.4.1.161.19.3.1.1.94.0	Integer
rfOLTrap.0	.1.3.6.1.4.1.161.19.3.1.1.95.0	Integer
rfOLThreshold.0	.1.3.6.1.4.1.161.19.3.1.1.96.0	Integer
rfOLEnable.0	.1.3.6.1.4.1.161.19.3.1.1.97.0	Integer
linkTestLUID.0	.1.3.6.1.4.1.161.19.3.1.2.1.1.0	Integer
linkTestDuration.0	.1.3.6.1.4.1.161.19.3.1.2.1.2.0	Integer
linkTestAction.0	.1.3.6.1.4.1.161.19.3.1.2.1.3.0	Integer
linkTestPktLength.0	.1.3.6.1.4.1.161.19.3.1.2.1.4.0	Integer
testLUID.0	.1.3.6.1.4.1.161.19.3.1.2.2.1.0	Integer

linkTestStatus.0	.1.3.6.1.4.1.161.19.3.1.2.2.2.0	OctetString
linkTestError.0	.1.3.6.1.4.1.161.19.3.1.2.2.3.0	OctetString
testDuration.0	.1.3.6.1.4.1.161.19.3.1.2.2.4.0	Integer
downLinkRate.0	.1.3.6.1.4.1.161.19.3.1.2.2.5.0	Integer
upLinkRate.0	.1.3.6.1.4.1.161.19.3.1.2.2.6.0	Integer
downLinkEff.0	.1.3.6.1.4.1.161.19.3.1.2.2.7.0	Integer
maxDwnLinkIndex.0	.1.3.6.1.4.1.161.19.3.1.2.2.8.0	Integer
actDwnLinkIndex.0	.1.3.6.1.4.1.161.19.3.1.2.2.9.0	Integer
expDwnFragCount.0	.1.3.6.1.4.1.161.19.3.1.2.2.10.0	Gauge
actDwnFragCount.0	.1.3.6.1.4.1.161.19.3.1.2.2.11.0	Gauge
upLinkEff.0	.1.3.6.1.4.1.161.19.3.1.2.2.12.0	Integer
expUpFragCount.0	.1.3.6.1.4.1.161.19.3.1.2.2.13.0	Gauge
actUpFragCount.0	.1.3.6.1.4.1.161.19.3.1.2.2.14.0	Gauge
maxUpLinkIndex.0	.1.3.6.1.4.1.161.19.3.1.2.2.15.0	Integer
actUpLinkIndex.0	.1.3.6.1.4.1.161.19.3.1.2.2.16.0	Integer
whispGPSStats.0	.1.3.6.1.4.1.161.19.3.1.3.1.0	Integer
gpsSyncSource.0	.1.3.6.1.4.1.161.19.3.1.3.2.0	OctetString
gpsSyncStatus.0	.1.3.6.1.4.1.161.19.3.1.3.3.0	OctetString
gpsTrackingMode.0	.1.3.6.1.4.1.161.19.3.1.3.4.0	OctetString
gpsTime.0	.1.3.6.1.4.1.161.19.3.1.3.5.0	OctetString
gpsDate.0	.1.3.6.1.4.1.161.19.3.1.3.6.0	OctetString
gpsSatellitesTracked.0	.1.3.6.1.4.1.161.19.3.1.3.7.0	OctetString
gpsSatellitesVisible.0	.1.3.6.1.4.1.161.19.3.1.3.8.0	OctetString
gpsHeight.0	.1.3.6.1.4.1.161.19.3.1.3.9.0	OctetString
gpsAntennaConnection.0	.1.3.6.1.4.1.161.19.3.1.3.10.0	OctetString
gpsLatitude.0	.1.3.6.1.4.1.161.19.3.1.3.11.0	OctetString
gpsLongitude.0	.1.3.6.1.4.1.161.19.3.1.3.12.0	OctetString
gpsInvalidMsg.0	.1.3.6.1.4.1.161.19.3.1.3.13.0	OctetString
gpsRestartCount.0	.1.3.6.1.4.1.161.19.3.1.3.14.0	Integer
gpsReInitCount.0	.1.3.6.1.4.1.161.19.3.1.3.15.0	Integer

gpsReceiverInfo.0	.1.3.6.1.4.1.161.19.3.1.3.16.0	OctetString
linkLUID.2	.1.3.6.1.4.1.161.19.3.1.4.1.1.2	Integer
linkDescr.2	.1.3.6.1.4.1.161.19.3.1.4.1.2.2	OctetString
linkPhysAddress.2	.1.3.6.1.4.1.161.19.3.1.4.1.3.2	OctetString
linkMtu.2	.1.3.6.1.4.1.161.19.3.1.4.1.4.2	Integer
linkSpeed.2	.1.3.6.1.4.1.161.19.3.1.4.1.5.2	Gauge
linkInOctets.2	.1.3.6.1.4.1.161.19.3.1.4.1.7.2	Counter32
linkInUcastPkts.2	.1.3.6.1.4.1.161.19.3.1.4.1.8.2	Counter32
linkInNUcastPkts.2	.1.3.6.1.4.1.161.19.3.1.4.1.9.2	Counter32
linkInDiscards.2	.1.3.6.1.4.1.161.19.3.1.4.1.10.2	Counter32
linkInError.2	.1.3.6.1.4.1.161.19.3.1.4.1.11.2	Counter32
linkInUnknownProtos.2	.1.3.6.1.4.1.161.19.3.1.4.1.12.2	Counter32
linkOutOctets.2	.1.3.6.1.4.1.161.19.3.1.4.1.13.2	Counter32
linkOutUcastPkts.2	.1.3.6.1.4.1.161.19.3.1.4.1.14.2	Counter32
linkOutNUcastPkts.2	.1.3.6.1.4.1.161.19.3.1.4.1.15.2	Counter32
linkOutDiscards.2	.1.3.6.1.4.1.161.19.3.1.4.1.16.2	Counter32
linkOutError.2	.1.3.6.1.4.1.161.19.3.1.4.1.17.2	Counter32
linkOutQLen.2	.1.3.6.1.4.1.161.19.3.1.4.1.18.2	Gauge
linkSessState.2	.1.3.6.1.4.1.161.19.3.1.4.1.19.2	Integer
linkESN.2	.1.3.6.1.4.1.161.19.3.1.4.1.20.2	OctetString
linkRSSI.2	.1.3.6.1.4.1.161.19.3.1.4.1.21.2	Integer
linkAveJitter.2	.1.3.6.1.4.1.161.19.3.1.4.1.22.2	Gauge
linkLastJitter.2	.1.3.6.1.4.1.161.19.3.1.4.1.23.2	Gauge
linkAirDelay.2	.1.3.6.1.4.1.161.19.3.1.4.1.24.2	Integer
linkRegCount.2	.1.3.6.1.4.1.161.19.3.1.4.1.25.2	Integer
linkReRegCount.2	.1.3.6.1.4.1.161.19.3.1.4.1.26.2	Integer
linkTimeOut.2	.1.3.6.1.4.1.161.19.3.1.4.1.27.2	Integer
linkLastRSSI.2	.1.3.6.1.4.1.161.19.3.1.4.1.28.2	Integer
sessionCount.2	.1.3.6.1.4.1.161.19.3.1.4.1.29.2	Integer

softwareVersion.2	.1.3.6.1.4.1.161.19.3.1.4.1.30.2	OctetString
softwareBootVersion.2	.1.3.6.1.4.1.161.19.3.1.4.1.31.2	OctetString
fpgaVersion.2	.1.3.6.1.4.1.161.19.3.1.4.1.32.2	OctetString
linkSiteName.2	.1.3.6.1.4.1.161.19.3.1.4.1.33.2	OctetString
avgPowerLevel.2	.1.3.6.1.4.1.161.19.3.1.4.1.34.2	OctetString
lastPowerLevel.2	.1.3.6.1.4.1.161.19.3.1.4.1.35.2	OctetString
sesDownLinkRate.2	.1.3.6.1.4.1.161.19.3.1.4.1.36.2	Integer
sesDownLinkLimit.2	.1.3.6.1.4.1.161.19.3.1.4.1.37.2	Integer
sesUpLinkRate.2	.1.3.6.1.4.1.161.19.3.1.4.1.38.2	Integer
sesUpLinkLimit.2	.1.3.6.1.4.1.161.19.3.1.4.1.39.2	Integer
adaptRate.2	.1.3.6.1.4.1.161.19.3.1.4.1.40.2	OctetString
sesLoUpCIR.2	.1.3.6.1.4.1.161.19.3.1.4.1.41.2	Integer
sesLoDownCIR.2	.1.3.6.1.4.1.161.19.3.1.4.1.42.2	Integer
sesHiUpCIR.2	.1.3.6.1.4.1.161.19.3.1.4.1.43.2	Integer
sesHiDownCIR.2	.1.3.6.1.4.1.161.19.3.1.4.1.44.2	Integer
platformVer.2	.1.3.6.1.4.1.161.19.3.1.4.1.45.2	Integer
smSessionTmr.2	.1.3.6.1.4.1.161.19.3.1.4.1.46.2	TimeTicks
smSessionSeqNumMismatch.2	.1.3.6.1.4.1.161.19.3.1.4.1.47.2	Counter32
dataVCNum.2	.1.3.6.1.4.1.161.19.3.1.4.1.48.2	Integer
hiPriQEn.2	.1.3.6.1.4.1.161.19.3.1.4.1.49.2	Integer
dataVCNumHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.50.2	Integer
linkInOctetsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.51.2	Counter32
linkInUcastPktsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.52.2	Counter32
linkInNUcastPktsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.53.2	Counter32
linkInDiscardsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.54.2	Counter32
linkInErrorHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.55.2	Counter32
linkInUnknownProtosHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.56.2	Counter32
linkOutOctetsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.57.2	Counter32
linkOutUcastPktsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.58.2	Counter32
linkOutNUcastPktsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.59.2	Counter32

linkOutDiscardsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.60.2	Counter32
linkOutErrorHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.61.2	Counter32
vcQOverflow.2	.1.3.6.1.4.1.161.19.3.1.4.1.62.2	Counter32
vcQOverflowHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.63.2	Counter32
p7p8HiPriQEn.2	.1.3.6.1.4.1.161.19.3.1.4.1.64.2	Integer
p7p8HiPriQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.65.2	Counter32
linkAirDelayns.2	.1.3.6.1.4.1.161.19.3.1.4.1.66.2	Integer
linkManagementIP.2	.1.3.6.1.4.1.161.19.3.1.4.1.69.2	IpAddress
radiusReplyMsg.2	.1.3.6.1.4.1.161.19.3.1.4.1.75.2	OctetString
radiusFramedIPAddress.2	.1.3.6.1.4.1.161.19.3.1.4.1.77.2	IpAddress
radiusFramedIPNetmask.2	.1.3.6.1.4.1.161.19.3.1.4.1.78.2	IpAddress
radiusDefaultGateway.2	.1.3.6.1.4.1.161.19.3.1.4.1.79.2	IpAddress
regCount.0	.1.3.6.1.4.1.161.19.3.1.7.1.0	Gauge
gpsStatus.0	.1.3.6.1.4.1.161.19.3.1.7.2.0	OctetString
radioTxGainAp.0	.1.3.6.1.4.1.161.19.3.1.7.4.0	Integer
dataSlotDwn.0	.1.3.6.1.4.1.161.19.3.1.7.5.0	Integer
dataSlotUp.0	.1.3.6.1.4.1.161.19.3.1.7.6.0	Integer
numCtrSlot.0	.1.3.6.1.4.1.161.19.3.1.7.12.0	Gauge
maxRegSMCount.0	.1.3.6.1.4.1.161.19.3.1.7.18.0	Integer
systemTime.0	.1.3.6.1.4.1.161.19.3.1.7.19.0	OctetString
lastNTPTime.0	.1.3.6.1.4.1.161.19.3.1.7.20.0	OctetString
regulatoryStatus.0	.1.3.6.1.4.1.161.19.3.1.7.21.0	OctetString
dhcpRlyAgntStat-reqRecvd.0	.1.3.6.1.4.1.161.19.3.1.7.22.0	Counter32
dhcpRlyAgntStat-reqRelayed.0	.1.3.6.1.4.1.161.19.3.1.7.23.0	Counter32
dhcpRlyAgntStat-reqDiscards.0	.1.3.6.1.4.1.161.19.3.1.7.24.0	Counter32
dhcpRlyAgntStat-respRecvd.0	.1.3.6.1.4.1.161.19.3.1.7.25.0	Counter32
dhcpRlyAgntStat-respRelayed.0	.1.3.6.1.4.1.161.19.3.1.7.26.0	Counter32
dhcpRlyAgntStat-respDiscards.0	.1.3.6.1.4.1.161.19.3.1.7.27.0	Counter32
dhcpRlyAgntStat-untrustedDiscards.0	.1.3.6.1.4.1.161.19.3.1.7.28.0	Counter32

dhcpRlyAgntStat-maxHopDiscards.0	.1.3.6.1.4.1.161.19.3.1.7.29.0	Counter32
dhcpRlyAgntStat-pktTooBig.0	.1.3.6.1.4.1.161.19.3.1.7.30.0	Counter32
dhcpRlyAgntStat-invalidGiaddrDiscards.0	.1.3.6.1.4.1.161.19.3.1.7.31.0	Counter32
regFailureCount.0	.1.3.6.1.4.1.161.19.3.1.7.32.0	Counter32
ntpLogSNMP.0	.1.3.6.1.4.1.161.19.3.1.7.33.0	OctetString
uGPSPowerStatus.0	.1.3.6.1.4.1.161.19.3.1.7.34.0	OctetString
rfOutDiscardRate.0	.1.3.6.1.4.1.161.19.3.1.7.35.0	Integer
ntpDomainNameAppend.0	.1.3.6.1.4.1.161.19.3.1.9.1.0	Integer
ntpServer1.0	.1.3.6.1.4.1.161.19.3.1.9.2.0	OctetString
ntpServer2.0	.1.3.6.1.4.1.161.19.3.1.9.3.0	OctetString
ntpServer3.0	.1.3.6.1.4.1.161.19.3.1.9.4.0	OctetString
dhcprDomainNameAppend.0	.1.3.6.1.4.1.161.19.3.1.9.5.0	Integer
dhcprServer.0	.1.3.6.1.4.1.161.19.3.1.9.6.0	OctetString
authDomainNameAppend.0	.1.3.6.1.4.1.161.19.3.1.9.7.0	Integer
authServer1.0	.1.3.6.1.4.1.161.19.3.1.9.8.0	OctetString
authServer2.0	.1.3.6.1.4.1.161.19.3.1.9.9.0	OctetString
authServer3.0	.1.3.6.1.4.1.161.19.3.1.9.10.0	OctetString
authServer4.0	.1.3.6.1.4.1.161.19.3.1.9.11.0	OctetString
authServer5.0	.1.3.6.1.4.1.161.19.3.1.9.12.0	OctetString
acctDomainNameAppend.0	.1.3.6.1.4.1.161.19.3.1.9.13.0	Integer

SM and BH Timing Slave Objects

The objects that the Canopy Enterprise MIB defines for each SM and BH Timing Slave are listed in Table 73.

Table 73: Canopy Enterprise MIB objects for SMs and BH timing slaves

Name	OID	valueType
rfScanList.0	.1.3.6.1.4.1.161.19.3.2.1.1.0	OctetString
powerUpMode.0	.1.3.6.1.4.1.161.19.3.2.1.2.0	Integer
lanIpSm.0	.1.3.6.1.4.1.161.19.3.2.1.3.0	IpAddress

lanMaskSm.0	.1.3.6.1.4.1.161.19.3.2.1.4.0	IpAddress
defaultGwSm.0	.1.3.6.1.4.1.161.19.3.2.1.5.0	IpAddress
networkAccess.0	.1.3.6.1.4.1.161.19.3.2.1.6.0	Integer
authKeySm.0	.1.3.6.1.4.1.161.19.3.2.1.7.0	OctetString
enable8023link.0	.1.3.6.1.4.1.161.19.3.2.1.8.0	Integer
authKeyOption.0	.1.3.6.1.4.1.161.19.3.2.1.9.0	Integer
timingPulseGated.0	.1.3.6.1.4.1.161.19.3.2.1.10.0	Integer
naptPrivateIP.0	.1.3.6.1.4.1.161.19.3.2.1.11.0	IpAddress
naptPrivateSubnetMask.0	.1.3.6.1.4.1.161.19.3.2.1.12.0	IpAddress
naptPublicIP.0	.1.3.6.1.4.1.161.19.3.2.1.13.0	IpAddress
naptPublicSubnetMask.0	.1.3.6.1.4.1.161.19.3.2.1.14.0	IpAddress
naptPublicGatewayIP.0	.1.3.6.1.4.1.161.19.3.2.1.15.0	IpAddress
naptRFPublicIP.0	.1.3.6.1.4.1.161.19.3.2.1.16.0	IpAddress
naptRFPublicSubnetMask.0	.1.3.6.1.4.1.161.19.3.2.1.17.0	IpAddress
naptRFPublicGateway.0	.1.3.6.1.4.1.161.19.3.2.1.18.0	IpAddress
naptEnable.0	.1.3.6.1.4.1.161.19.3.2.1.19.0	Integer
arpCacheTimeout.0	.1.3.6.1.4.1.161.19.3.2.1.20.0	Integer
tcpGarbageCollectTmout.0	.1.3.6.1.4.1.161.19.3.2.1.21.0	Integer
udpGarbageCollectTmout.0	.1.3.6.1.4.1.161.19.3.2.1.22.0	Integer
dhcpServerEnable.0	.1.3.6.1.4.1.161.19.3.2.1.24.0	Integer
dhcpServerLeaseTime.0	.1.3.6.1.4.1.161.19.3.2.1.25.0	Integer
dhcpIPStart.0	.1.3.6.1.4.1.161.19.3.2.1.26.0	IpAddress
dnsAutomatic.0	.1.3.6.1.4.1.161.19.3.2.1.27.0	Integer
prefferedDNSIP.0	.1.3.6.1.4.1.161.19.3.2.1.28.0	IpAddress
alternateDNSIP.0	.1.3.6.1.4.1.161.19.3.2.1.29.0	IpAddress
dmzIP.0	.1.3.6.1.4.1.161.19.3.2.1.30.0	IpAddress
dmzEnable.0	.1.3.6.1.4.1.161.19.3.2.1.31.0	Integer
dhcpNumIPsToLease.0	.1.3.6.1.4.1.161.19.3.2.1.32.0	Integer
pppoeFilter.0	.1.3.6.1.4.1.161.19.3.2.1.33.0	Integer

smbFilter.0	.1.3.6.1.4.1.161.19.3.2.1.34.0	Integer
snmpFilter.0	.1.3.6.1.4.1.161.19.3.2.1.35.0	Integer
userP1Filter.0	.1.3.6.1.4.1.161.19.3.2.1.36.0	Integer
userP2Filter.0	.1.3.6.1.4.1.161.19.3.2.1.37.0	Integer
userP3Filter.0	.1.3.6.1.4.1.161.19.3.2.1.38.0	Integer
allOtherIpFilter.0	.1.3.6.1.4.1.161.19.3.2.1.39.0	Integer
arpFilter.0	.1.3.6.1.4.1.161.19.3.2.1.41.0	Integer
allOthersFilter.0	.1.3.6.1.4.1.161.19.3.2.1.42.0	Integer
userDefinedPort1.0	.1.3.6.1.4.1.161.19.3.2.1.43.0	Integer
port1TCPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.44.0	Integer
port1UDPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.45.0	Integer
userDefinedPort2.0	.1.3.6.1.4.1.161.19.3.2.1.46.0	Integer
port2TCPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.47.0	Integer
port2UDPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.48.0	Integer
userDefinedPort3.0	.1.3.6.1.4.1.161.19.3.2.1.49.0	Integer
port3TCPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.50.0	Integer
port3UDPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.51.0	Integer
bootpcFilter.0	.1.3.6.1.4.1.161.19.3.2.1.52.0	Integer
bootpsFilter.0	.1.3.6.1.4.1.161.19.3.2.1.53.0	Integer
ip4MultFilter.0	.1.3.6.1.4.1.161.19.3.2.1.54.0	Integer
ingressVID.0	.1.3.6.1.4.1.161.19.3.2.1.55.0	Integer
lowPriorityUplinkCIR.0	.1.3.6.1.4.1.161.19.3.2.1.56.0	Integer
lowPriorityDownlinkCIR.0	.1.3.6.1.4.1.161.19.3.2.1.57.0	Integer
hiPriorityChannel.0	.1.3.6.1.4.1.161.19.3.2.1.58.0	Integer
hiPriorityUplinkCIR.0	.1.3.6.1.4.1.161.19.3.2.1.59.0	Integer
hiPriorityDownlinkCIR.0	.1.3.6.1.4.1.161.19.3.2.1.60.0	Integer
upLnkDataRate.0	.1.3.6.1.4.1.161.19.3.2.1.62.0	Integer
upLnkLimit.0	.1.3.6.1.4.1.161.19.3.2.1.63.0	Integer
dwnLnkDataRate.0	.1.3.6.1.4.1.161.19.3.2.1.64.0	Integer
dwnLnkLimit.0	.1.3.6.1.4.1.161.19.3.2.1.65.0	Integer

ipAccessFilterEnable.0	.1.3.6.1.4.1.161.19.3.2.1.68.0	Integer
allowedIPAccess1.0	.1.3.6.1.4.1.161.19.3.2.1.69.0	IpAddress
allowedIPAccess2.0	.1.3.6.1.4.1.161.19.3.2.1.70.0	IpAddress
allowedIPAccess3.0	.1.3.6.1.4.1.161.19.3.2.1.71.0	IpAddress
rfDhcpState.0	.1.3.6.1.4.1.161.19.3.2.1.72.0	Integer
bCastMIR.0	.1.3.6.1.4.1.161.19.3.2.1.73.0	Integer
smLEDModeFlag.0	.1.3.6.1.4.1.161.19.3.2.1.75.0	Integer
ethAccessEnable.0	.1.3.6.1.4.1.161.19.3.2.1.76.0	Integer
pppoeEnable.0	.1.3.6.1.4.1.161.19.3.2.1.77.0	Integer
pppoeAuthenticationType.0	.1.3.6.1.4.1.161.19.3.2.1.78.0	Integer
pppoeAccessConcentrator.0	.1.3.6.1.4.1.161.19.3.2.1.79.0	OctetString
pppoeServiceName.0	.1.3.6.1.4.1.161.19.3.2.1.80.0	OctetString
pppoeUserName.0	.1.3.6.1.4.1.161.19.3.2.1.81.0	OctetString
pppoePassword.0	.1.3.6.1.4.1.161.19.3.2.1.82.0	OctetString
pppoeTCPMSSClampEnable.0	.1.3.6.1.4.1.161.19.3.2.1.83.0	Integer
pppoeMTUOverrideEnable.0	.1.3.6.1.4.1.161.19.3.2.1.84.0	Integer
pppoeMTUOverrideValue.0	.1.3.6.1.4.1.161.19.3.2.1.85.0	Integer
pppoeTimerType.0	.1.3.6.1.4.1.161.19.3.2.1.86.0	Integer
pppoeTimeoutPeriod.0	.1.3.6.1.4.1.161.19.3.2.1.87.0	Integer
timedSpectrumAnalysisDuration.0	.1.3.6.1.4.1.161.19.3.2.1.88.0	Integer
spectrumAnalysisOnBoot.0	.1.3.6.1.4.1.161.19.3.2.1.89.0	Integer
spectrumAnalysisAction.0	.1.3.6.1.4.1.161.19.3.2.1.90.0	Integer
pppoeConnectOD.0	.1.3.6.1.4.1.161.19.3.2.1.91.0	Integer
pppoeDisconnectOD.0	.1.3.6.1.4.1.161.19.3.2.1.92.0	Integer
natConnectionType.0	.1.3.6.1.4.1.161.19.3.2.1.94.0	Integer
wanPingReplyEnable.0	.1.3.6.1.4.1.161.19.3.2.1.95.0	Integer
packetFilterDirection.0	.1.3.6.1.4.1.161.19.3.2.1.96.0	Integer
colorCode2.0	.1.3.6.1.4.1.161.19.3.2.1.97.0	Integer
colorCodepriority2.0	.1.3.6.1.4.1.161.19.3.2.1.98.0	Integer

colorCode3.0	.1.3.6.1.4.1.161.19.3.2.1.99.0	Integer
colorCodepriority3.0	.1.3.6.1.4.1.161.19.3.2.1.100.0	Integer
colorCode4.0	.1.3.6.1.4.1.161.19.3.2.1.101.0	Integer
colorCodepriority4.0	.1.3.6.1.4.1.161.19.3.2.1.102.0	Integer
colorCode5.0	.1.3.6.1.4.1.161.19.3.2.1.103.0	Integer
colorCodepriority5.0	.1.3.6.1.4.1.161.19.3.2.1.104.0	Integer
colorCode6.0	.1.3.6.1.4.1.161.19.3.2.1.105.0	Integer
colorCodepriority6.0	.1.3.6.1.4.1.161.19.3.2.1.106.0	Integer
colorCode7.0	.1.3.6.1.4.1.161.19.3.2.1.107.0	Integer
colorCodepriority7.0	.1.3.6.1.4.1.161.19.3.2.1.108.0	Integer
colorCode8.0	.1.3.6.1.4.1.161.19.3.2.1.109.0	Integer
colorCodepriority8.0	.1.3.6.1.4.1.161.19.3.2.1.110.0	Integer
colorCode9.0	.1.3.6.1.4.1.161.19.3.2.1.111.0	Integer
colorCodepriority9.0	.1.3.6.1.4.1.161.19.3.2.1.112.0	Integer
colorCode10.0	.1.3.6.1.4.1.161.19.3.2.1.113.0	Integer
colorCodepriority10.0	.1.3.6.1.4.1.161.19.3.2.1.114.0	Integer
natDNSProxyEnable.0	.1.3.6.1.4.1.161.19.3.2.1.115.0	Integer
allIpv4Filter.0	.1.3.6.1.4.1.161.19.3.2.1.116.0	Integer
spectrumAnalysisDisplay.0	.1.3.6.1.4.1.161.19.3.2.1.117.0	Integer
eapPeerAAAServerCommonName.0	.1.3.6.1.4.1.161.19.3.2.1.126.0	OctetString
sessionStatus.0	.1.3.6.1.4.1.161.19.3.2.2.1.0	OctetString
rssi.0	.1.3.6.1.4.1.161.19.3.2.2.2.0	Integer
jitter.0	.1.3.6.1.4.1.161.19.3.2.2.3.0	Gauge
airDelay.0	.1.3.6.1.4.1.161.19.3.2.2.4.0	Gauge
radioTxGainSm.0	.1.3.6.1.4.1.161.19.3.2.2.6.0	Integer
calibrationStatus.0	.1.3.6.1.4.1.161.19.3.2.2.7.0	OctetString
radioDbm.0	.1.3.6.1.4.1.161.19.3.2.2.8.0	OctetString
registeredToAp.0	.1.3.6.1.4.1.161.19.3.2.2.9.0	OctetString
dhcpCip.0	.1.3.6.1.4.1.161.19.3.2.2.10.0	IpAddress
dhcpSip.0	.1.3.6.1.4.1.161.19.3.2.2.11.0	IpAddress

dhcpClientLease.0	.1.3.6.1.4.1.161.19.3.2.2.12.0	TimeTicks
dhcpCSMask.0	.1.3.6.1.4.1.161.19.3.2.2.13.0	IpAddress
dhcpDfltRterIP.0	.1.3.6.1.4.1.161.19.3.2.2.14.0	IpAddress
dhcpcdns1.0	.1.3.6.1.4.1.161.19.3.2.2.15.0	IpAddress
dhcpcdns2.0	.1.3.6.1.4.1.161.19.3.2.2.16.0	IpAddress
dhcpcdns3.0	.1.3.6.1.4.1.161.19.3.2.2.17.0	IpAddress
dhcpDomName.0	.1.3.6.1.4.1.161.19.3.2.2.18.0	OctetString
adaptRate.0	.1.3.6.1.4.1.161.19.3.2.2.20.0	OctetString
radioDbmInt.0	.1.3.6.1.4.1.161.19.3.2.2.21.0	Integer
radioTxPwr.0	.1.3.6.1.4.1.161.19.3.2.2.23.0	OctetString
activeRegion.0	.1.3.6.1.4.1.161.19.3.2.2.24.0	OctetString
snmpBerLevel.0	.1.3.6.1.4.1.161.19.3.2.2.25.0	Integer
nbBitsRcvd.0	.1.3.6.1.4.1.161.19.3.2.2.26.0	Counter64
nbPriBitsErr.0	.1.3.6.1.4.1.161.19.3.2.2.27.0	Counter32
nbSndBitsErr.0	.1.3.6.1.4.1.161.19.3.2.2.28.0	Counter32
minRSSI.0	.1.3.6.1.4.1.161.19.3.2.2.32.0	Integer
maxRSSI.0	.1.3.6.1.4.1.161.19.3.2.2.33.0	Integer
minJitter.0	.1.3.6.1.4.1.161.19.3.2.2.34.0	Gauge
maxJitter.0	.1.3.6.1.4.1.161.19.3.2.2.35.0	Gauge
smSessionTimer.0	.1.3.6.1.4.1.161.19.3.2.2.36.0	TimeTicks
pppoeSessionStatus.0	.1.3.6.1.4.1.161.19.3.2.2.37.0	OctetString
pppoeSessionID.0	.1.3.6.1.4.1.161.19.3.2.2.38.0	Integer
pppoeIPCPAddress.0	.1.3.6.1.4.1.161.19.3.2.2.39.0	IpAddress
pppoeMTUOverrideEn.0	.1.3.6.1.4.1.161.19.3.2.2.40.0	Integer
pppoeMTUValue.0	.1.3.6.1.4.1.161.19.3.2.2.41.0	Integer
pppoeTimerTypeValue.0	.1.3.6.1.4.1.161.19.3.2.2.42.0	Integer
pppoeTimeoutValue.0	.1.3.6.1.4.1.161.19.3.2.2.43.0	Integer
pppoeDNSServer1.0	.1.3.6.1.4.1.161.19.3.2.2.44.0	IpAddress
pppoeDNSServer2.0	.1.3.6.1.4.1.161.19.3.2.2.45.0	IpAddress

pppoeControlBytesSent.0	.1.3.6.1.4.1.161.19.3.2.2.46.0	Counter32
pppoeControlBytesReceived.0	.1.3.6.1.4.1.161.19.3.2.2.47.0	Counter32
pppoeDataBytesSent.0	.1.3.6.1.4.1.161.19.3.2.2.48.0	Counter32
pppoeDataBytesReceived.0	.1.3.6.1.4.1.161.19.3.2.2.49.0	Counter32
pppoeEnabledStatus.0	.1.3.6.1.4.1.161.19.3.2.2.50.0	Integer
pppoeTCPMSSClampEnableStatus.0	.1.3.6.1.4.1.161.19.3.2.2.51.0	Integer
pppoeACNameStatus.0	.1.3.6.1.4.1.161.19.3.2.2.52.0	OctetString
pppoeSvcNameStatus.0	.1.3.6.1.4.1.161.19.3.2.2.53.0	OctetString
pppoeSessUptime.0	.1.3.6.1.4.1.161.19.3.2.2.54.0	TimeTicks
primaryBERDisplay.0	.1.3.6.1.4.1.161.19.3.2.2.55.0	OctetString
secondaryBERDisplay.0	.1.3.6.1.4.1.161.19.3.2.2.56.0	OctetString
totalBERDisplay.0	.1.3.6.1.4.1.161.19.3.2.2.57.0	OctetString
minRadioDbm.0	.1.3.6.1.4.1.161.19.3.2.2.58.0	Integer
maxRadioDbm.0	.1.3.6.1.4.1.161.19.3.2.2.59.0	Integer
pppoeSessIdleTime.0	.1.3.6.1.4.1.161.19.3.2.2.60.0	TimeTicks
airDelayns.0	.1.3.6.1.4.1.161.19.3.2.2.64.0	Gauge
currentColorCode.0	.1.3.6.1.4.1.161.19.3.2.2.65.0	Integer
currentColorCodePri.0	.1.3.6.1.4.1.161.19.3.2.2.66.0	Integer
currentChanFreq.0	.1.3.6.1.4.1.161.19.3.2.2.67.0	Gauge
linkQualityBeacon.0	.1.3.6.1.4.1.161.19.3.2.2.68.0	OctetString
dhcpServerPktXmt.0	.1.3.6.1.4.1.161.19.3.2.2.72.0	Counter32
dhcpServerPktRcv.0	.1.3.6.1.4.1.161.19.3.2.2.73.0	Counter32
dhcpServerPktToss.0	.1.3.6.1.4.1.161.19.3.2.2.74.0	Counter32
receiveFragmentsModulationPercentage.0	.1.3.6.1.4.1.161.19.3.2.2.86.0	OctetString
signalToNoiseRatioSM.0	.1.3.6.1.4.1.161.19.3.2.2.95.0	Integer
protocol.1	.1.3.6.1.4.1.161.19.3.2.5.1.2.1	Integer
protocol.2	.1.3.6.1.4.1.161.19.3.2.5.1.2.2	Integer
protocol.3	.1.3.6.1.4.1.161.19.3.2.5.1.2.3	Integer
protocol.4	.1.3.6.1.4.1.161.19.3.2.5.1.2.4	Integer
protocol.5	.1.3.6.1.4.1.161.19.3.2.5.1.2.5	Integer

protocol.6	.1.3.6.1.4.1.161.19.3.2.5.1.2.6	Integer
protocol.7	.1.3.6.1.4.1.161.19.3.2.5.1.2.7	Integer
protocol.8	.1.3.6.1.4.1.161.19.3.2.5.1.2.8	Integer
protocol.9	.1.3.6.1.4.1.161.19.3.2.5.1.2.9	Integer
protocol.10	.1.3.6.1.4.1.161.19.3.2.5.1.2.10	Integer
port.1	.1.3.6.1.4.1.161.19.3.2.5.1.3.1	Integer
port.2	.1.3.6.1.4.1.161.19.3.2.5.1.3.2	Integer
port.3	.1.3.6.1.4.1.161.19.3.2.5.1.3.3	Integer
port.4	.1.3.6.1.4.1.161.19.3.2.5.1.3.4	Integer
port.5	.1.3.6.1.4.1.161.19.3.2.5.1.3.5	Integer
port.6	.1.3.6.1.4.1.161.19.3.2.5.1.3.6	Integer
port.7	.1.3.6.1.4.1.161.19.3.2.5.1.3.7	Integer
port.8	.1.3.6.1.4.1.161.19.3.2.5.1.3.8	Integer
port.9	.1.3.6.1.4.1.161.19.3.2.5.1.3.9	Integer
port.10	.1.3.6.1.4.1.161.19.3.2.5.1.3.10	Integer
localIp.1	.1.3.6.1.4.1.161.19.3.2.5.1.4.1	IpAddress
localIp.2	.1.3.6.1.4.1.161.19.3.2.5.1.4.2	IpAddress
localIp.3	.1.3.6.1.4.1.161.19.3.2.5.1.4.3	IpAddress
localIp.4	.1.3.6.1.4.1.161.19.3.2.5.1.4.4	IpAddress
localIp.5	.1.3.6.1.4.1.161.19.3.2.5.1.4.5	IpAddress
localIp.6	.1.3.6.1.4.1.161.19.3.2.5.1.4.6	IpAddress
localIp.7	.1.3.6.1.4.1.161.19.3.2.5.1.4.7	IpAddress
localIp.8	.1.3.6.1.4.1.161.19.3.2.5.1.4.8	IpAddress
localIp.9	.1.3.6.1.4.1.161.19.3.2.5.1.4.9	IpAddress
localIp.10	.1.3.6.1.4.1.161.19.3.2.5.1.4.10	IpAddress
whispTranslationTableMacAddr.1	.1.3.6.1.4.1.161.19.3.2.6.1.2.1	OctetString
whispTranslationTableMacAddr.2	.1.3.6.1.4.1.161.19.3.2.6.1.2.2	OctetString
whispTranslationTableIpAddr.1	.1.3.6.1.4.1.161.19.3.2.6.1.3.1	IpAddress
whispTranslationTableIpAddr.2	.1.3.6.1.4.1.161.19.3.2.6.1.3.2	IpAddress

whispTranslationTableAge.1	.1.3.6.1.4.1.161.19.3.2.6.1.4.1	Counter32
whispTranslationTableAge.2	.1.3.6.1.4.1.161.19.3.2.6.1.4.2	Counter32
certIndex.1	.1.3.6.1.4.1.161.19.3.2.7.1.1.1.1	Integer
certIndex.2	.1.3.6.1.4.1.161.19.3.2.7.1.1.1.2	Integer
cert.1	.1.3.6.1.4.1.161.19.3.2.7.1.1.2.1	Integer
cert.2	.1.3.6.1.4.1.161.19.3.2.7.1.1.2.2	Integer
action.1	.1.3.6.1.4.1.161.19.3.2.7.1.1.3.1	Integer
action.2	.1.3.6.1.4.1.161.19.3.2.7.1.1.3.2	Integer
certificateDN.1	.1.3.6.1.4.1.161.19.3.2.7.1.1.4.1	OctetString
certificateDN.2	.1.3.6.1.4.1.161.19.3.2.7.1.1.4.2	OctetString
numAuthCerts.0	.1.3.6.1.4.1.161.19.3.2.7.2.0	Integer
authenticationEnforce.0	.1.3.6.1.4.1.161.19.3.2.7.3.0	Integer
phase1.0	.1.3.6.1.4.1.161.19.3.2.7.4.0	Integer
phase2.0	.1.3.6.1.4.1.161.19.3.2.7.5.0	Integer
authOuterId.0	.1.3.6.1.4.1.161.19.3.2.7.6.0	OctetString
authPassword.0	.1.3.6.1.4.1.161.19.3.2.7.7.0	OctetString
authUsername.0	.1.3.6.1.4.1.161.19.3.2.7.8.0	OctetString
useRealm.0	.1.3.6.1.4.1.161.19.3.2.7.9.0	Integer
realm.0	.1.3.6.1.4.1.161.19.3.2.7.10.0	OctetString

Interface Designations in SNMP

SNMP identifies the ports of the module as follows:

- Interface 1 represents the Ethernet interface of the module. To monitor the status of Interface 1 is to monitor the traffic on the Ethernet interface.
- Interface 2 represents the RF interface of the module. To monitor the status of Interface 2 is to monitor the traffic on the RF interface.

These interfaces can be viewed on the NMS through definitions that are provided in the standard MIB files.

Traps Provided in the Canopy Enterprise MIB

Canopy modules provide the following SNMP traps for automatic notifications to the NMS:

- coldStart, which signals that the SNMPv2 element is reinitializing itself and that its configuration may have been altered.
- warmStart, which signals that the SNMPv2 element is reinitializing such that its configuration is unaltered.
- authenticationFailure, which signals that the SNMPv2 element has received a protocol message that is not properly authenticated (contingent on the snmpEnableAuthenTraps object setting).
- linkDown, as defined in RFC 1573
- linkUp, as defined in RFC 1573
- egpNeighborLoss, as defined in RFC 1213
- whispGPSInSync, which signals a transition from not synchronized to synchronized.
- whispGPSOutSync, which signals a transition from synchronized to not synchronized.
- whispRegComplete, which signals registration completed.
- whispRegLost, which signals registration lost.
- whispRadarDetected, which signals that the one-minute scan has been completed, radar has been detected, and the radio will shutdown.
- whispRadarEnd, which signals that the one-minute scan has been completed, radar *has not* been detected, and the radio will resume normal operation.

NOTE:
The PTP 300, 400, 500 600 series wireless Ethernet bridges do not support the traps listed above.

MIB Viewers

Any of several commercially available MIB viewers can facilitate management of these objects through SNMP. Some are available as open source software. Cambium does not endorse, support, or discourage the use of any these viewers.

MIB viewers are available and/or described at the following web sites:

- http://ns3.ndgsoftware.com/Products/NetBoy30/mibbrowser.html
- http://www.adventnet.com/products/snmputilities/

- http://www.dart.com/samples/mib.asp
- http://www.edge-technologies.com/webFiles/products/nvision/index.cfm
- http://www.ipswitch.com/products/whatsup/monitoring.html
- http://www.koshna.com/products/KMB/index.asp
- http://www.mg-soft.si/mgMibBrowserPE.html
- http://www.mibexplorer.com
- http://www.netmechanica.com/mibbrowser.html
- http://www.networkview.com
- http://www.newfreeware.com/search.php3?q=MIB+browser
- http://www.nudesignteam.com/walker.html
- http://www.oidview.com/oidview.html
- http://www.solarwinds.net/Tools
- http://www.stargus.com/solutions/xray.html
- http://www.totilities.com/Products/MibSurfer/MibSurfer.htm

Chapter 26: Using the Canopy Network Updater Tool (CNUT)

The Canopy Network Updater Tool (CNUT) manages and automates the software and firmware upgrade process for a Canopy radio, CMMmicro, or CMM4 (but not its 14-port switch) across the network. This eliminates the need for an administrator to visit each radio in the network (or each AP while using the Autoupdate feature) to upgrade the modules.

CNUT Functions

The Canopy Network Updater Tool

- automatically discovers all network elements
- executes a UDP command that initiates and terminates the Autoupdate mode within APs. This command is both secure and convenient:
  - For security, the AP accepts this command from only the IP address that you specify in the Configuration page of the AP.
  - For convenience, Network Updater automatically sets this Configuration parameter in the APs to the IP address of the Network Updater server when the server performs any of the update commands.
- allows you to choose among updating
  - your entire network.
  - only elements that you select.
  - only network branches that you select.
- provides a Script Engine that you can use with any script that
  - you define.
  - Cambium supplies.

Network Element Groups

With the Canopy Network Updater Tool, you can identify element groups composed of network elements that you select. Identifying these element groups

- organizes the display of elements (for example, by region or by AP cluster).
- allows you to
  - perform an operation on all elements in the group simultaneously.

- set group-level defaults for telnet or ftp password access and SNMP Community String (defaults that can be overridden in an individual element when necessary).

If you have both FSK and OFDM modules in your network, then you must either ensure that they all run Release 9.4.2 or that you select these two types of modules into separate element groups because they are not running on the same software.

Network Layers

A typical network contains multiple layers of elements, each layer lying farther from the Point of Presence. For example, SMs are behind an AP and thus, in this context, at a lower layer than the AP. Correctly portraying these layers in Network Updater is essential so that Network Updater can perform radio and AP cluster upgrades in an appropriate order.

IMPORTANT!
Correct layer information ensures that Network Updater does not command an AP that is behind another AP/SM pair (such as in a remote AP installation) to perform an upgrade at the same time as the SM that is feeding the AP. If this occurs, then the remote AP loses network connection during the upgrade (when the SM in front of the AP completes its upgrade and reboots).

Script Engine

Script Engine is the capability in Network Updater that executes any user-defined script against any network element or element group. This capability is useful for network management, especially for scripts that you repetitively execute across your network.

The Autodiscovery capability in Network Updater finds all of your network elements. This comprehensive discovery

- ensures that, when you intend to execute a script against *all* elements, the script is indeed executed against *all* elements.
- maintains master lists of elements (element groups) against which you selectively execute scripts.

The following scripts are included with CNUT:

- AP Data Import from BAM
- AP Data Export to BAM
- Set Autoupdate Address on APs
- Set SNMP Accessibility
- Reset Unit

Software Dependencies for CNUT

CNUT functionality requires

- one of the following operating systems
  - Windows® 2000
  - Windows Server 2003
  - Windows XP or XP Professional
  - Windows 7
  - Red Hat Enterprise Linux (32-bit) Version 4 or 5
- Java™ Runtime Version 2.0 or later (installed by the CNUT installation tool)

CNUT Download

CNUT can be downloaded together with each system release that supports CNUT. Software for these system releases is available from http://www.cambiumnetworks.com/support/planning/index.php?cat=3&type=1/ as either

- a `.zip` file for use without the CNUT application.
- a `.pkg` file that the CNUT application can open.

Chapter 27: Using Informational Tabs in the GUI

Viewing General Status (All)

See

- General Status Tab of the AP on Page 212.
- General Status Tab of the SM on Page 207.
- General Status Tab of the BHM on Page 229.
- Beginning the Test of Point-to-Point Links on Page 223.

Viewing Session Status (AP, BHM)

The Session Status tab in the Home page provides information about each SM that has registered to the AP. This information is useful for managing and troubleshooting a system. This tab also includes the current active values on each SM for MIR, CIR, and VLAN, as well as the source of these values, representing the SM itself, BAM, or the AP and cap.

- (SM) – QoS/VLAN parameters are derived from the SM's settings
- (APCAP) – QoS/VLAN parameters are derived from the AP's settings, including any keyed capping (for radios capped at 4 Mbps, 10 Mbps, or 20 Mbps)
- (D) – QoS/VLAN parameters are retrieved from the device, due to failed retrieval from the AAA or WM server.
- (AAA) – QoS/VLAN parameters are retrieved from the RADIUS server
- (BAM) – QoS/VLAN parameters are retrieved from a WM BAM server

An example of the Session Status tab is displayed in Figure 158.

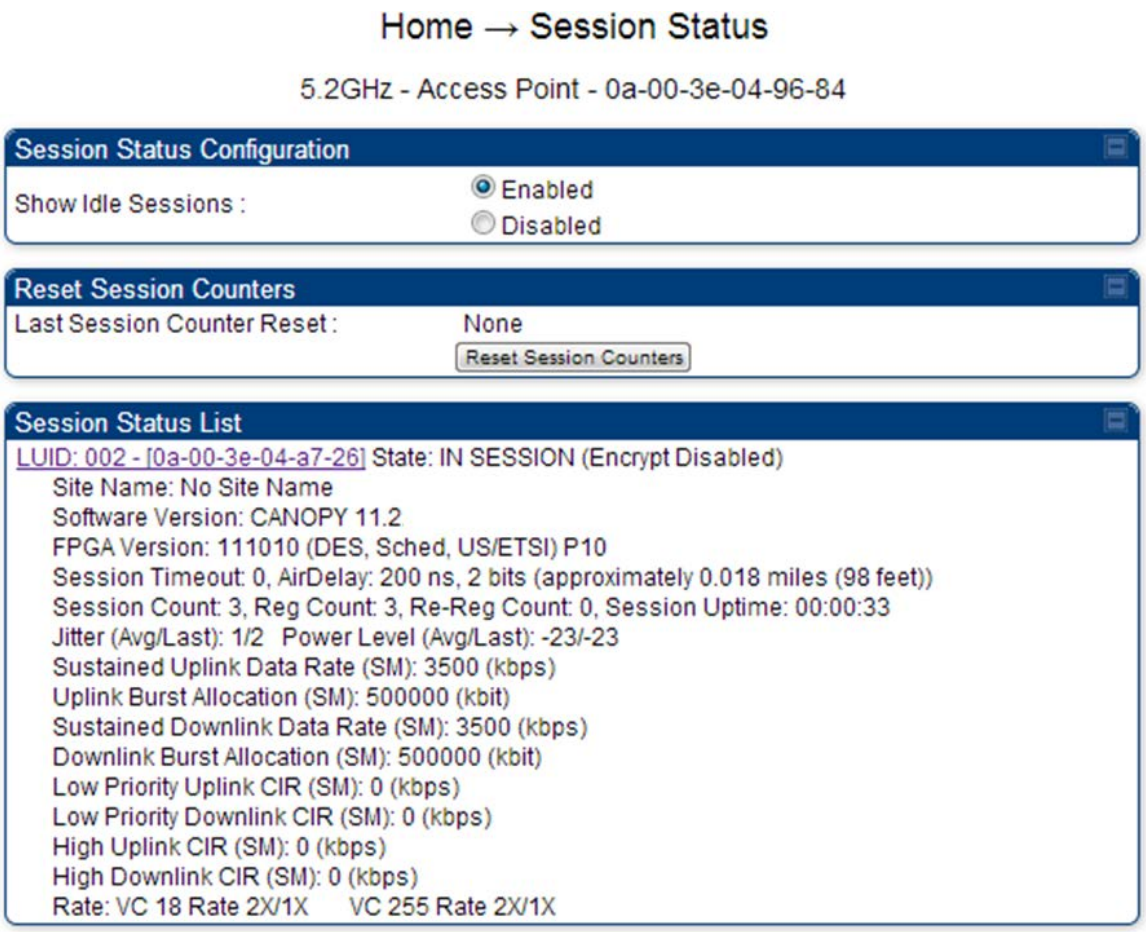

Home → Session Status
5.2GHz - Access Point - 0a-00-3e-04-96-84
Session Status Configuration
Show Idle Sessions :
Enabled
Disabled
Reset Session Counters
Last Session Counter Reset :
None
Reset Session Counters
Session Status List
LUID: 002 - [0a-00-3e-04-a7-26] State: IN SESSION (Encrypt Disabled)
Site Name: No Site Name
Software Version: CANOPY 11.2
FPGA Version: 111010 (DES, Sched, US/ETSI) P10
Session Timeout: 0, AirDelay: 200 ns, 2 bits (approximately 0.018 miles (98 feet))
Session Count: 3, Reg Count: 3, Re-Reg Count: 0, Session Uptime: 00:00:33
Jitter (Avg/Last): 1/2 Power Level (Avg/Last): -23/-23
Sustained Uplink Data Rate (SM): 3500 (kbps)
Uplink Burst Allocation (SM): 500000 (kbit)
Sustained Downlink Data Rate (SM): 3500 (kbps)
Downlink Burst Allocation (SM): 500000 (kbit)
Low Priority Uplink CIR (SM): 0 (kbps)
Low Priority Downlink CIR (SM): 0 (kbps)
High Uplink CIR (SM): 0 (kbps)
High Downlink CIR (SM): 0 (kbps)
Rate: VC 18 Rate 2X/1X VC 255 Rate 2X/1X

Figure 158: Session Status tab data, example

An additional example and explanations of the fields on this tab are provided in Session Status Tab of the AP on Page 200.

Viewing Remote Subscribers (AP, BHM)

See

- Remote Subscribers Tab of the AP on Page 206.
- Continuing the Test of Point-to-Point Links on Page 228.

Interpreting Messages in the Event Log (All)

Each line in the Event Log of a module Home page begins with a time and date stamp. However, some of these lines wrap as a combined result of window width, browser preferences, and line length. You may find this tab easiest to use if you widen the window until all lines are shown as beginning with the time and date stamp.

Time and Date Stamp

The time and date stamp reflect either

- GPS time and date directly or indirectly received from the CMM.
- the running time and date that you have set in the Time & Date web page.

NOTE:
In the Time & Date web page, if you have left any time field or date field unset and clicked the **Set Time and Date** button, then the time and date default to 00:00:00 UT : 01/01/00.

A reboot causes the preset time to pause or, in some cases, to run in reverse. Additionally, a power cycle resets the running time and date to the default 00:00:00 UT : 01/01/00. Thus, whenever either a reboot or a power cycle has occurred, you should reset the time and date in the Time & Date web page of any module that is not set to receive sync.

Event Log Data Collection

The collection of event data continues through reboots and power cycles. When the buffer allowance for event log data is reached, the system adds new data into the log and discards an identical amount of the oldest data.

Each line that contains the expression WatchDog flags an event that was both

- considered by the system software to have been an exception
- recorded in the *preceding* line.

Conversely, a Fatal Error() message flags an event that is recorded in the *next* line. Some exceptions and fatal errors may be significant and require either operator action or technical support.

An example portion of Event Log data is displayed in Figure 159. In this figure (unlike in the Event Log web page)

- lines are alternately highlighted to show the varying length of wrapped lines.

- the types of event messages (which follow the time and date stamps and the file and line references) are underscored as quoted in Table 74 and Table 75.

Home → Event Log
5.2GHz - Access Point - 0a-00-3e-04-96-84
System Event Log
12/31/2010 : 20:15:47 CST :
******System Startup******
System Reset Exception -- Watchdog Reset Cur ExtInt 0 Max ExtInt 0 Cur DecInt 0 Max DecInt 0 Cur Sync 0 Max Sync 0 Cur LED 2 Max LED 1 Cur WDOG 0 Max WDOG 1 Cur EthXcvr 0 Max EthXcvr 1 Cur FEC 0 Max FEC 0 Cur FPGA 0 Max FPGA 0 Cur FrmLoc 0 Max FrmLoc 0 Cur WatchDog 33 Max WatchDog 33 RTMLogStats 0 AAState 0
Software Version : CANOPY 11.2 AP-DES
Board Type : P10
Device Setting : AP
FPGA Version : 111010
FPGA Features : DES, Sched, US/ETSI
Clear Event Log

Figure 159: Event Log tab data, example

Messages that Flag Abnormal Events

The messages listed in Table 74 flag abnormal events and, case by case, may signal the need for corrective action or technical support. See Troubleshooting on Page 570.

Table 74: Event Log messages for abnormal events

Event Message	Meaning
Expected LUID = *6* Actual LUID = *7*	Something is interfering with the control messaging of the module. Also ensure that you are using shielded cables to minimize interference. Consider trying different frequency options to eliminate or reduce interference.
FatalError()	The event recorded on the line immediately beneath this message triggered the Fatal Error().
Loss of GPS Sync Pulse	Module has lost GPS sync signal.
Machine Check Exception	This is a symptom of a possible hardware failure. If this is a recurring message, begin the RMA process for the module.
RcvFrmNum = *0x00066d* ExpFrmNum = *0x000799*	Something is interfering with the control messaging of the module. Also ensure that you are using shielded cables to minimize interference. Consider trying different frequency options to eliminate or reduce interference.
System Reset Exception -- External Hard Reset	The unit lost power or was power cycled.
System Reset Exception -- External Hard Reset WatchDog	The event recorded on the preceding line triggered this WatchDog message.

Messages that Flag Normal Events

The messages listed in Table 75 record normal events and typically *do not* signal a need for any corrective action or technical support.

Table 75: Event Log messages for normal events

Event Message	Meaning
Acquired GPS Sync Pulse.	Module has acquired GPS sync signal.
FPGA Features	Type of encryption.
FPGA Version	FPGA (JBC) version in the module.
GPS Date/Time Set	Module is now on GPS time.
PowerOn reset from Telnet command line	Reset command was issued from a `telnet` session.
Reboot from Webpage	Module was rebooted from management interface.
Software Version	The software release and authentication method for the unit.
System Log Cleared	Event log was manually cleared.

Viewing the Network Interface Tab (All)

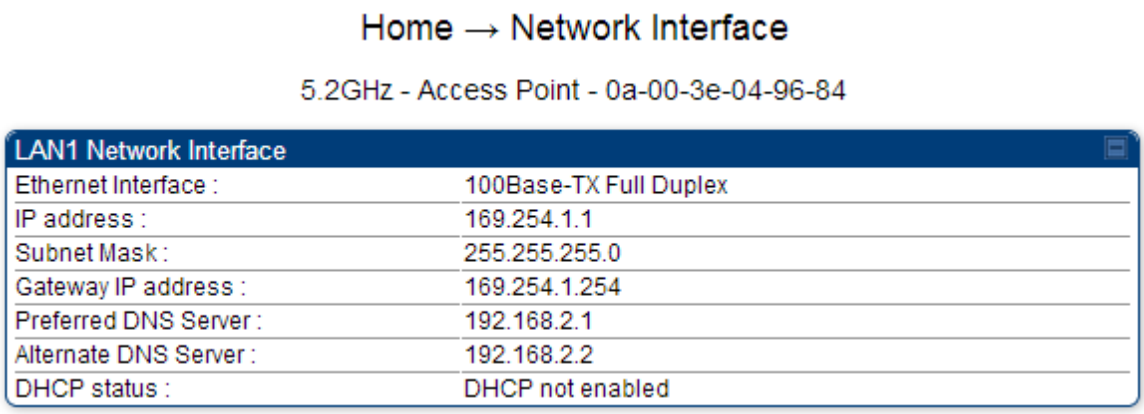

Home → Network Interface
5.2GHz - Access Point - 0a-00-3e-04-96-84
LAN1 Network Interface
Ethernet Interface : 100Base-TX Full Duplex
IP address : 169.254.1.1
Subnet Mask : 255.255.255.0
Gateway IP address : 169.254.1.254
Preferred DNS Server : 192.168.2.1
Alternate DNS Server : 192.168.2.2
DHCP status : DHCP not enabled

Figure 160: Network Interface tab of AP, example

In any module, the LAN1 Network Interface section of this tab displays the defined Internet Protocol scheme for the Ethernet interface to the module. In slave devices, this tab also provides an RF Public Network Interface section, which displays the Internet Protocol scheme defined for network access through the master device (AP or BHM).

Viewing the Layer 2 Neighbors Tab (All)

An example of the Layer 2 Neighbors tab is shown in Figure 161.

Figure 161: Layer 2 Neighbors log, example

Viewing the Scheduler Tab (All)

Statistics for the Scheduler are displayed as shown below.

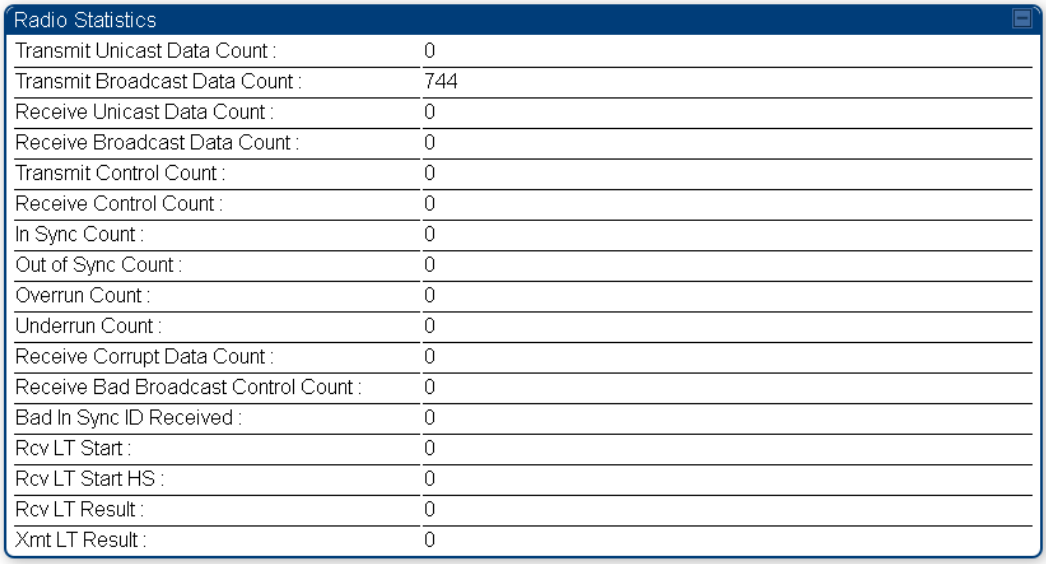

Radio Statistics
Transmit Unicast Data Count : 0
Transmit Broadcast Data Count : 744
Receive Unicast Data Count : 0
Receive Broadcast Data Count : 0
Transmit Control Count : 0
Receive Control Count : 0
In Sync Count : 0
Out of Sync Count : 0
Overrun Count : 0
Underrun Count : 0
Receive Corrupt Data Count : 0
Receive Bad Broadcast Control Count : 0
Bad In Sync ID Received : 0
Rcv LT Start : 0
Rcv LT Start HS : 0
Rcv LT Result : 0
Xmt LT Result : 0

Figure 162: Scheduler tab of the AP

Event Message	Meaning
Transmit Unicast Data Count	The total amount of unicast packets transmitted from the radio

Event Message	Meaning
Transmit Broadcast Data Count	The total amount of broadcast packets transmitted from the radio
Receive Unicast Data Count	The total amount of unicast packets received by the radio
Receive Broadcast Data Count	The total amount of broadcast packets received by the radio
Transmit Control Count	The amount of radio control type messages transmitted (registration requests and grants, power adjust, etc.).
Receive Control Count	The amount of radio control type messages received (registration requests and grants, power adjust, etc.).
In Sync Count	Number of times the radio has acquired sync. In the case of an AP generating sync this is when generated sync has been locked, or if GPS synchronization is used it is number of times GPS sync acquired. For the SM, it is the number of times the SM successfully obtained sync with an AP.
Out of Sync Count	Number of times the radio lost same sync lock.
Overrun Count	Number of times FPGA frame has overrun its TX Frame
Underrun Count	Number of times FPGAs TX Frame aborted prematurely.
Receive Corrupt Data Count	Number of times a corrupt fragment has been received at the FPGA.
Receive Bad Broadcast Control Count	Number of times the radio has received an invalid control message via broadcast (SM only).
Rcv LT Start	Number of Link Test Start messages received. A remote radio has requested that this radio start a link test to it.
Rcv LT Start HS	Number of Link Test Start Handshake messages received. This radio requested that a remote radio start a link test and the remote radio has sent a handshake back acknowledging the start.
Rcv LT Result	This radio received Link Test results from the remote radio under test. When this radio initiates a link test, the remote radio will send its results to this radio for display.
Xmt LT Result	This radio transmitted its link test results to the remote radio under test. When the remote radio initiates a link test, this radio must send its results to the remote radio for display there.

List of Registration Failures (AP, BHM)

The SM Registration Failures tab identifies SMs that have recently attempted and failed to register to this AP. With its time stamps, these instances may suggest that a new or transient source of interference exists.

Registration Failures Statistics
Number of Registration Grant Failures : 1
Most Recent Registration Failure List
MAC : 0a-00-3e-04-a7-26 AAA Session Retry 12/31/2010 : 19:23:30 CST : Status : 17 Flag : 0

Figure 163: SM Registration Failures tab of the AP

Interpreting Data in the Bridging Table (All)

If NAT (network address translation) is not active on the SM, then the Bridging Table tab provides the MAC address of all devices that are attached to registered SMs (identified by LUIDs). The bridging table allows data to be sent to the correct module as follows:

- For the AP, the uplink is from RF to Ethernet. Thus, when a packet arrives in the *RF* interface to the AP, the AP reads the MAC address from the inbound packet and creates a bridging table entry of the source MAC address on the other end of the *RF* interface.
- For the SM, the uplink is from Ethernet to RF. Thus, when a packet arrives in the *Ethernet* interface to one of these modules, the module reads the MAC address from the inbound packet and creates a bridging table entry of the source MAC address on the other end of the *Ethernet* interface.

Bridging Table
Mac:0A003EA00175 DestLUID:258 Age:-1 Hash:0981 Ent:02
Mac:1A003EA00175 DestLUID:259 Age:-1 Hash:0981 Ent:02
Used: 2 BridgeFree: 4094 BridgeFullErr: 0

Figure 164: Bridging Table tab of the AP

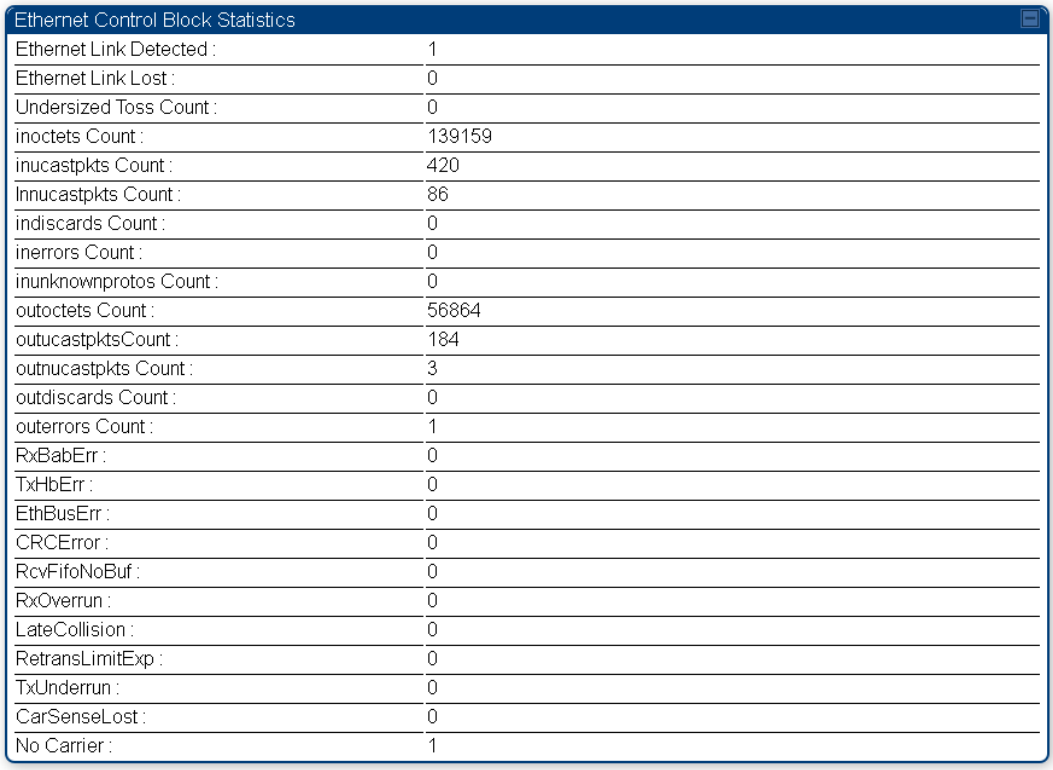
Translation Table (SM)

When Translation Bridging is enabled in the AP, each SM keeps a table mapping MAC addresses of devices attached to the AP to IP addresses, as otherwise the mapping of end-user MAC addresses to IP addresses is lost. (When Translation Bridging is enabled, an AP modifies all uplink traffic originating from registered SMs such that the source MAC address of every packet will be changed to that of the SM which bridged the packet in the uplink direction.)

Figure 165: Translation Table tab of the SM

Interpreting Data in the Ethernet Tab (All)

The Ethernet tab of the Statistics web page reports TCP throughput and error information for the Ethernet connection of the module.



Ethernet Control Block Statistics	
Ethernet Link Detected :	1
Ethernet Link Lost :	0
Undersized Toss Count :	0
inoctets Count :	139159
inucastpkts Count :	420
Innucastpkts Count :	86
indiscards Count :	0
inerrors Count :	0
inunknownprotos Count :	0
outoctets Count :	56864
outucastpktsCount :	184
outnucastpkts Count :	3
outdiscards Count :	0
outerrors Count :	1
RxBabErr :	0
TxHbErr :	0
EthBusErr :	0
CRCError :	0
RcvFifoNoBuf :	0
RxOverrun :	0
LateCollision :	0
RetransLimitExp :	0
TxUnderrun :	0
CarSenseLost :	0
No Carrier :	1

Figure 166: Ethernet tab of AP

The Ethernet tab displays the following fields.

Table 76: Ethernet tab attributes

Attribute	Meaning
Ethernet Link Detected	1 indicates that an Ethernet link is established to the radio, 0 indicates that no Ethernet link is established
Ethernet Link Lost	This field indicates a count of how many times the Ethernet link was lost.
Undersized Toss Count	This field indicates the number of packets that were too small to process and hence discarded.
inoctets Count	This field displays how many octets were received on the interface, including those that deliver framing information.
inucastpkts Count	This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
Innucastpkts Count	This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.
indiscards Count	This field displays how many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. (Some of these packets may have been discarded to increase buffer space.)
inerrors Count	This field displays how many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
inunknownprotos Count	This field displays how many inbound packets were discarded because of an unknown or unsupported protocol.
outoctets Count	This field displays how many octets were transmitted out of the interface, including those that deliver framing information.
outucastpkts Count	This field displays how many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.
outnucastpkts Count	This field displays how many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.

Attribute	Meaning
outdiscards Count	This field displays how many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)
outerrrors Count	This field displays how many outbound packets contained errors that prevented their transmission.
RxBabErr	This field displays how many receiver babble errors occurred.
TxHbErr	This field displays how many transmit heartbeat errors have occured.
EthBusErr	This field displays how many Ethernet bus errors occurred on the Ethernet controller.
CRCError	This field displays how many CRC errors occurred on the Ethernet controller.
RcvFifoNoBuf	This field displays the number of times no FIFO buffer space was able to be allocated
RxOverrun	This field displays how many receiver overrun errors occurred on the Ethernet controller.
Late Collision	This field displays how many late collisions occurred on the Ethernet controller. A normal collision occurs during the first 512 bits of the frame transmission. A collision that occurs after the first 512 bits is considered a late collision. ***IMPORTANT!*** A late collision is a serious network problem because the frame being transmitted is discarded. A late collision is most commonly caused by a mismatch between duplex configurations at the ends of a link segment.
RetransLimitExp	This field displays how many times the retransmit limit has expired.
TxUnderrun	This field displays how many transmission-underrun errors occurred on the Ethernet controller.
CarSenseLost	This field displays how many carrier sense lost errors occurred on the Ethernet controller.
No Carrier	This field displays how many no carrier errors occurred on the Ethernet controller.

Interpreting RF Control Block Statistics in the Radio Tab (All)

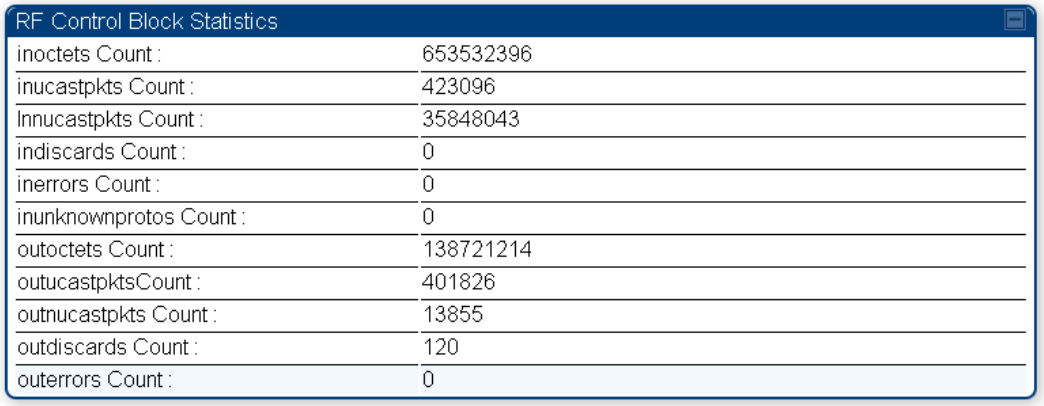


Figure 167: Radio tab of the Statistics page, SM

The Radio tab of the Statistics page displays the following fields.

Table 77: RF Control Block statistics attributes

Attribute	Meaning
inoctets Count	This field displays how many octets were received on the interface, including those that deliver framing information.
inucastpkts Count	This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
Innucastpkts Count	This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.

Attribute	Meaning
indiscards Count	This field displays how many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. This stat will be pegged whenever corrupt data is received by software or whenever the RF Software Bridge queue is full. Corrupt data is a very unusual event because all packets are CRC checked by hardware before being passed into software. The likely case for indiscards is if the RF bridge queue is full. If this is the case the radio is most likely PPS limited due to excessive small packet traffic or a problem at the Ethernet interface. If there is a problem at the Ethernet interface there is likely to be discards at the Ethernet as well.
inerrors Count	This field displays how many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
inunknownprotos Count	This field displays how many inbound packets were discarded because of an unknown or unsupported protocol.
outoctets Count	This field displays how many octets were transmitted out of the interface, including those that deliver framing information.
outucastpkts Count	This field displays how many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.
outnucastpkts Count	This field displays how many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.
outdiscards Count	This field displays how many outbound packets were discarded without errors that would have prevented their transmission. The link can be at capacity due to bandwidth being exceeded, poor RF links to the SMs, or sudden interference.
outerrrors Count	This field displays how many outbound packets contained errors that prevented their transmission.

Interpreting Data in the VLAN Tab (All)

The VLAN tab in the Statistics web page provides a list of the most recent packets that were filtered because of VLAN membership violations.

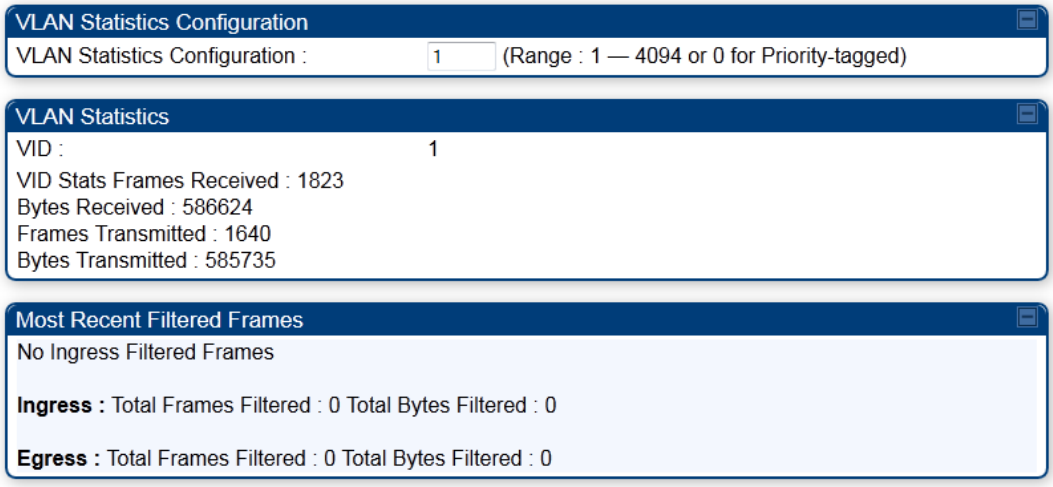

VLAN Statistics Configuration
VLAN Statistics Configuration :
1
(Range : 1 — 4094 or 0 for Priority-tagged)
VLAN Statistics
VID :
1
VID Stats Frames Received : 1823
Bytes Received : 586624
Frames Transmitted : 1640
Bytes Transmitted : 585735
Most Recent Filtered Frames
No Ingress Filtered Frames
Ingress : Total Frames Filtered : 0 Total Bytes Filtered : 0
Egress : Total Frames Filtered : 0 Total Bytes Filtered : 0

Figure 168: VLAN tab of the AP

Interpret entries under **Most Recent Filtered Frames** as follows:

- **Unknown**—This should not occur. Contact Technical Support.
- **Only Tagged**—The packet was filtered because the configuration is set to accept only packets that have an 802.1Q header, and this packet did not.
- **Ingress**—When the packet entered through the wired Ethernet interface, the packet was filtered because it indicated an incorrect VLAN membership.
- **Local Ingress**—When the packet was received from the local TCP/IP stack, the packet was filtered because it indicated an incorrect VLAN membership. This should not occur. Contact Technical Support.
- **Egress**—When the packet attempted to leave through the wired Ethernet interface, the packet was filtered because it indicated an incorrect VLAN membership.
- **Local Egress**—When the packet attempted to reach the local TCP/IP stack, the packet was filtered because it indicated an incorrect VLAN membership.

Viewing Data VC Statistics (All)

The Data VC Statistics tab displays information about the virtual channel (VC) used for data communications. The Data VC Statistics page provides individual stats for each VC which is currently allocated

Each SM will have one VC allocated to it for normal priority traffic and a second VC allocated to it if configured to use the high priority channel

If discard or error stats are seen on the RF Control Block stats page, this page should be consulted to determine if there is sector wide problem, or a problem with specific SM(s).

The in/out packets and octets are usual ifmib stats and represent the number of octets and packets passing from the software bridge into the RF hardware. Once a packet is passed to the RF hardware, it is guaranteed transmission over the RF link. If a packet fails transmission over the RF link, the session will be torn down. This is called a VC error.

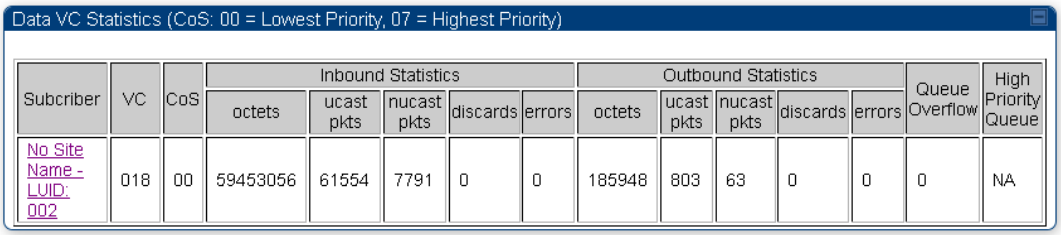


Figure 169: Data VC tab of the AP

The Data VC tab page displays the following fields.

Table 78: Data VC attributes

Attribute	Meaning
VC	This field displays the virtual channel number. Low priority channels start at VC18 and count up. High priority channels start at VC255 and count down. If one VC is displayed, the high-priority channel is disabled. If two are displayed, the high-priority channel is enabled.
CoS	This field displays the Class of Service for the virtual channel. The low priority channel is a CoS of 00, and the high priority channel is a CoS of 01. CoS of 02 through 07 are not currently used.
inoctets	This field displays how many octets were received on the interface, including those that deliver framing information.
inucastpkts	This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
innucastpkts	This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.

Attribute	Meaning
indiscards	This field displays how many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. Inbound discard statistics are incremented similar to the indiscards stat on the RF control block stats page. The sum of all data VC indiscards should be close to the RF control block in discards. If indiscards are evenly distributed across SMs, then the radio is PPS limited due to either excessive small packet transmissions, or a problem at the Ethernet link. If indiscards are contained to one or a few SMs, then there is likely a problem at or underneath the SM which is incrementing the count.
inerrors	This field displays how many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
outoctets	This field displays how many octets were transmitted out of the interface, including those that deliver framing information.
outucastpkts	This field displays how many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.
outnucastpkts	This field displays how many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.
outdiscards	This field displays how many outbound packets were discarded without errors that would have prevented their transmission. Outbound discard statistics are incremented if a VC is not active when a packet is ready to send. This is a rare condition.
outerrrors	This field displays how many outbound packets contained errors that prevented their transmission.
Queue Overflow	This is a count of packets that were discarded because the queue for the VC was already full. This stat will indicate congestion on the outbound RF link to a particular SM. If Queue Overflows are being seen across most or all SMs, then there is either an interferer local to the AP or the APs RF link is at capacity. If Queue Overflows are being seen at one or only a few SMs, then it is likely that there is a problem with those specific links whether it is insufficient signal strength, interferer, or a problem with the actual SM hardware.
High Priority Queue	P7/P8 Radio types only. This column indicates packets sent over the P7/P8 software-implemented high priority queue.

Viewing Summary Information in the Overload Tab (All)

The Overload tab displays statistics on packet overload and resultant packet discards. Unlike the other fields, the Total Packets Overload Count is expressed in only this tab. It is not a count of how many packets have been lost, but rather of how many discard events (packet loss bursts) have been detected due to overload condition.

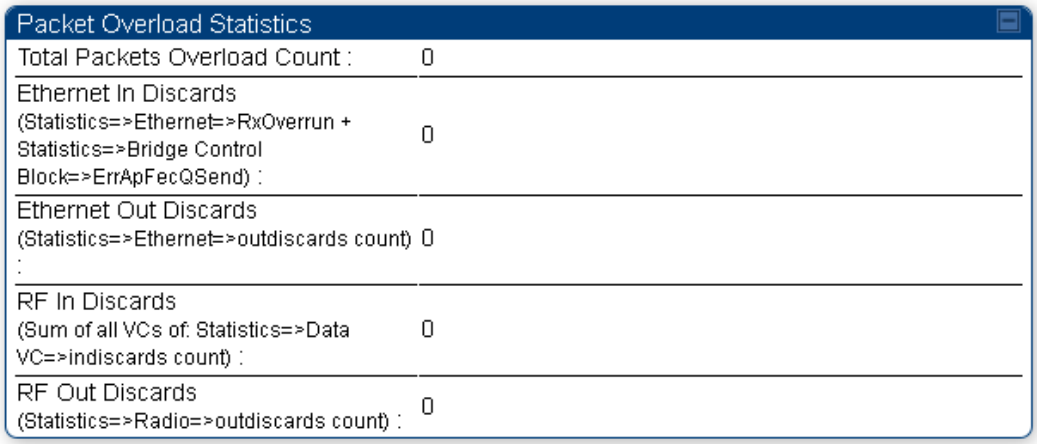

Packet Overload Statistics
Total Packets Overload Count :
0
Ethernet In Discards (Statistics=>Ethernet=>RxOverrun + Statistics=>Bridge Control Block=>ErrApFecQSend) :
0
Ethernet Out Discards (Statistics=>Ethernet=>outdiscards count) :
0
RF In Discards (Sum of all VCs of: Statistics=>Data VC=>indiscards count) :
0
RF Out Discards (Statistics=>Radio=>outdiscards count) :
0

Figure 170: Overload tab of the AP

Table 79: Overload tab attributes

Attribute	Meaning
Total Packets Overload Count	This field represents the sum of all RF and Ethernet in/out discards.
Ethernet In Discards	This field represents the number of packets tossed due to the Ethernet queue being full. If a climb in this stat accompanies a climb in RF Out Discards stat, then most likely the board is at RF capacity either due to traffic exceeding the RF pipe, or interference temporarily limiting the RF throughput. If this stat climbs without the RF Out Discards stat climbing, then the radio is most likely PPS limited.

Attribute	Meaning
Ethernet Out Discards	This field represents the number of packets tossed due to an Ethernet out overload. This stat should never climb in normal operation because the Ethernet link is much higher capacity than the RF link. If this stat is incrementing, then either the Ethernet link is established at a low speed (i.e. 10Mbps – half duplex), or there is a problem with cabling/Ethernet hardware.
RF In Discards	This field indicates the number of packets tossed due to no resources available within the radio to process them. This stat also should never be increasing because the system is designed to shed packets on the RF Out interface. If this stat is incrementing the board is most likely congested due to high PPS rate in combination with an Ethernet Out problem which will limit packet flow off the device.
RF Out Discards	This field indicates the number of packets tossed due to RF link at capacity. This stat will increase whenever the RF link is at capacity. When the internal FPGA RF input queue overflows, this stat is incremented. If this stat is seen to be incrementing at the AP, then the sector is congested. If seen at the SM, the number of control slots should be looked at to ensure that enough control slots are allocated to allow for bandwidth requests to be seen at the AP.

Viewing the DHCP Relay Tab (AP)

The DHCP Relay statistics tab displays requests and replies received, relayed, and discarded when the AP is configured as a DHCP relay. Typically, in a working DHCP realy configuration a one-to-one ratio is established between requests and replies that are received and relayed.

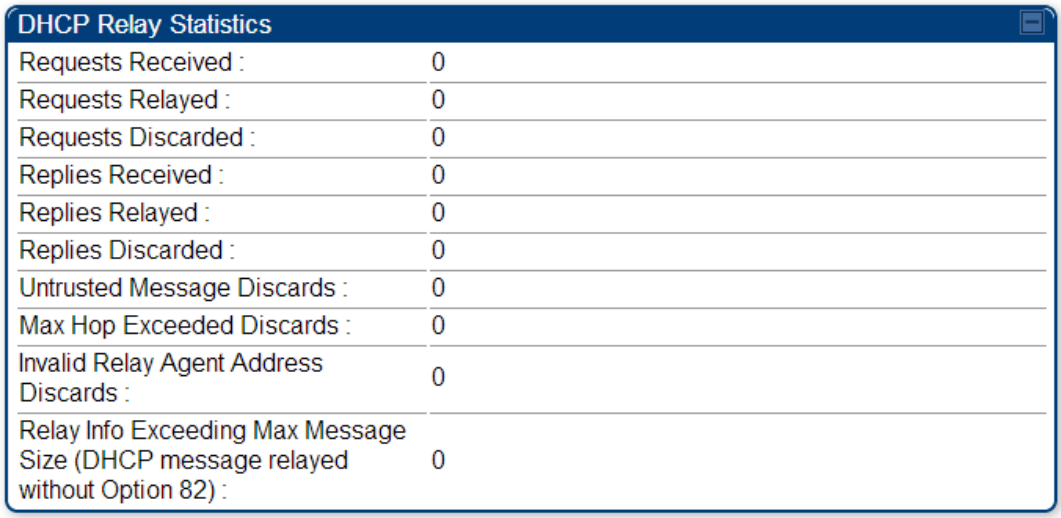

DHCP Relay Statistics
Requests Received : 0
Requests Relayed : 0
Requests Discarded : 0
Replies Received : 0
Replies Relayed : 0
Replies Discarded : 0
Untrusted Message Discards : 0
Max Hop Exceeded Discards : 0
Invalid Relay Agent Address Discards : 0
Relay Info Exceeding Max Message Size (DHCP message relayed without Option 82) : 0

Figure 171: DHCP Relay tab of the AP

Table 80: DHCP Relay attributes

Attribute	Meaning
Requests Received	This field represents the number of DHCP relay requests received by the AP.
Requests Relayed	This field represents the number of DHCP relay requests relayed by the AP.
Requests Discarded	This field represents the number of DHCP relay requests discarded by the AP due to errors in the request.
Replies Received	This field represents the number of DHCP relay replies received by the AP.
Replies Relayed	This field represents the number of DHCP relay replies relayed by the AP.
Replies Discarded	This field represents the number of DHCP relay replies discarded by the AP due to errors in the reply.
Untrusted Message Discards	This field indicates messages that were discarded because the message already contained Option 82 information with no Relay Agent specified.
Max Hop Exceeded Discards	This field indicates messages that have been relayed too many times, exceeding the max hop count (16).

Attribute	Meaning
Invalid Relay Agent Address Discards	This field indicates messages that have been discarded because the message relay agent address is already in place (relay agent address does not equal address of the AP).
Relay Info Exceeding Max Message Size (DHCP message relayed without Option 82)	This field indicates DHCP messages too large to fit Option 82 data. These messages are sent on without Option 82 information.

Viewing Filter Statistics (SM, BHS)

The Filter tab displays statistics on packets that have been filtered (dropped) due to the filters set on the Protocol Filtering tab.

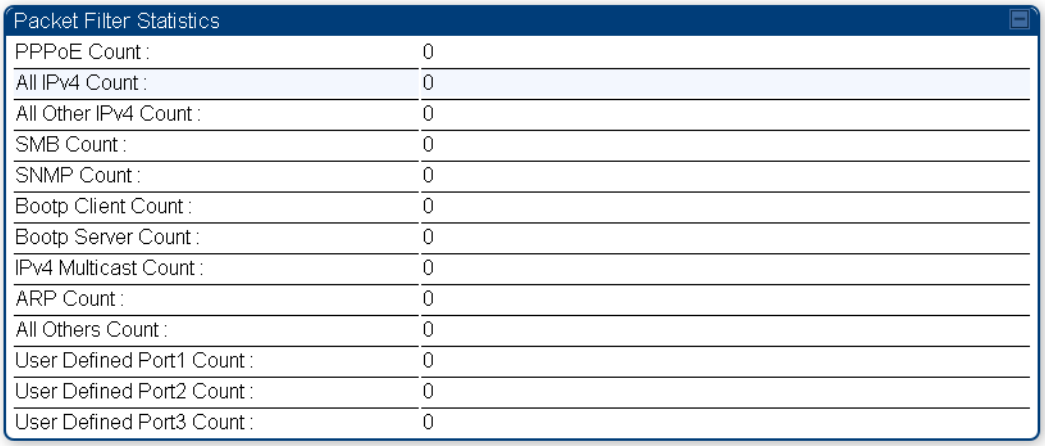

Packet Filter Statistics
PPPoE Count : 0
All IPv4 Count : 0
All Other IPv4 Count : 0
SMB Count : 0
SNMP Count : 0
Bootp Client Count : 0
Bootp Server Count : 0
IPv4 Multicast Count : 0
ARP Count : 0
All Others Count : 0
User Defined Port1 Count : 0
User Defined Port2 Count : 0
User Defined Port3 Count : 0

Figure 172: Filter tab of the SM

Viewing ARP Statistics (SM, BHS)

The ARP tab in an SM module correlated the IP address of the Ethernet-connected device to its MAC address and provides data about the connection.

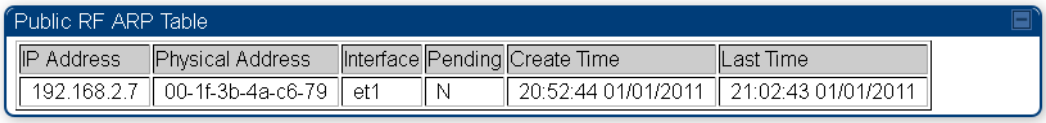


Figure 173: ARP tab of the SM

Viewing NAT Statistics (SM)

When NAT is enabled on an SM, statistics are kept on the Public and Private (WAN and LAN) sides of the NAT, and displayed on the NAT Stats tab.

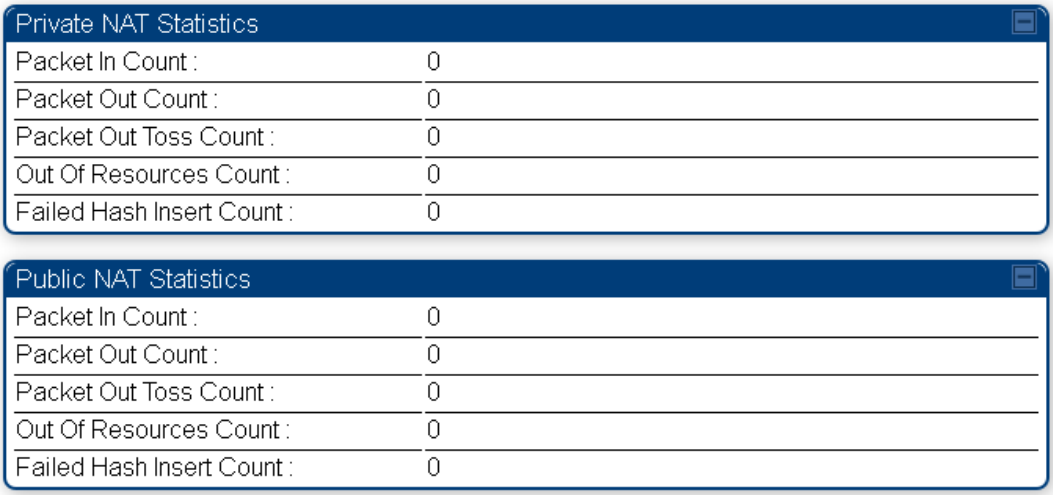

Private NAT Statistics
Packet In Count : 0
Packet Out Count : 0
Packet Out Toss Count : 0
Out Of Resources Count : 0
Failed Hash Insert Count : 0
Public NAT Statistics
Packet In Count : 0
Packet Out Count : 0
Packet Out Toss Count : 0
Out Of Resources Count : 0
Failed Hash Insert Count : 0

Figure 174: NAT Stats tab of the SM

Table 81 NAT Stats attributes

Attribute	Meaning
Private NAT Statistics, Packet In Count	This field represents the number of packets received on the SM's LAN/Ethernet interface

Attribute	Meaning
Private NAT Statistics, Packet Out Count	This field represents the number of packets sent from the SM's LAN/Ethernet interface
Private NAT Statistics, Packet Out Toss Count	This field represents the number of packets that we not sent from the SM's LAN/Ethernet interface due to addressing issues.
Private NAT Statistics, Out of Resources Count	This field represents the number of times the NAT table for the SM's LAN/Ethernet interfaces has been filled.
Private NAT Statistics, Failed Hash Insert Count	This field represents the number of times that the device failed to insert an address binding into the NAT hash table.
Public NAT Statistics, Packet In Count	This field represents the number of packets received on the SM's WAN/wireless interface
Public NAT Statistics, Packet Out Count	This field represents the number of packets sent from the SM's WAN/wireless interface
Public NAT Statistics, Out of Resources Count	This field represents the number of packets that we not sent from the SM's WAN/wireless interface due to addressing issues.
Public NAT Statistics, Failed Hash Insert Count	This field represents the number of times the NAT table for the SM's WAN/wireless interfaces has been filled.

Viewing NAT DHCP Statistics (SM)

When NAT is enabled on an SM with DHCP client (**DHCP** selected as the **Connection Type** of the WAN interface) and/or DHCP Server, statistics are kept for packets transmitted, received, and tossed, as well as a table of lease information for the DHCP server (Assigned IP Address, Hardware Address, and Lease Remained/State).

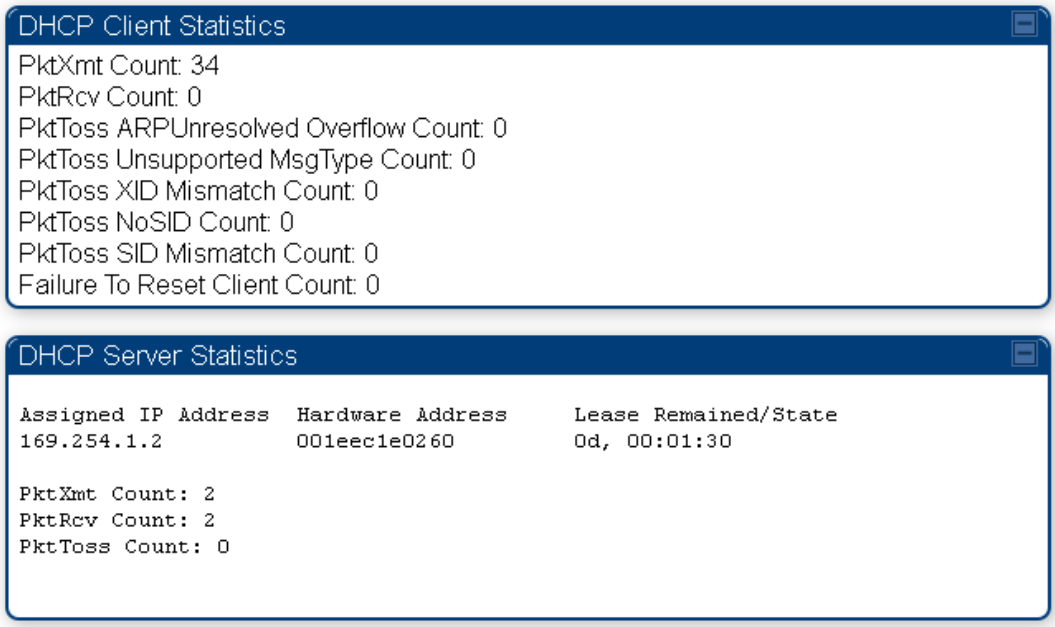

DHCP Client Statistics
PktXmt Count: 34
PktRcv Count: 0
PktToss ARPUnresolved Overflow Count: 0
PktToss Unsupported MsgType Count: 0
PktToss XID Mismatch Count: 0
PktToss NoSID Count: 0
PktToss SID Mismatch Count: 0
Failure To Reset Client Count: 0
DHCP Server Statistics
Assigned IP Address Hardware Address Lease Remained/State
169.254.1.2 001eec1e0260 0d, 00:01:30
PktXmt Count: 2
PktRcv Count: 2
PktToss Count: 0

Figure 175: NAT DHCP Statistics of the SM

Attribute	Meaning
PktXmt Count	This field represents the number of DHCP packets transmitted from the client
PktRcv Count	This field represents the number of DHCP packets received by the client
PktToss ARPUnresolved Overflow Count	This field represents the number of packets tossed due to failed attempts to resolve an IP address into a physical MAC address
PktToss Unsupported MsgType Count	This field represents the number of packets tossed due to the receipt of an unsupported message type (cannot be interpreted by DHCP client)

Attribute	Meaning
PktToss XID Mismatch Count	The field represents the number of packets that were tossed due to a transaction ID mismatch
PktToss NoSID Count	This field represents the number of packets that were tossed due to lack of a DHCP session ID
PktToss SIT Mismatch Count	This field represents the number of packets that were tossed due to a session ID mismatch
Failure to Reset Client Count	This field represents the number of times the DHCP client was unable to be reset (resulting in no IP address being served).

Interpreting Data in the GPS Status Page (AP, BHM)

The GPS Status tab is only displayed when the Sync Input is set to Sync to Received Signal (Timing Port), which is the configuration desired when connecting an AP to a CMM or UGPS.

The page displays information similar to that available on the web pages of a CMM, including Pulse Status, GPS Time and Date, Satellites Tracked, Available Satellites, Height, Latitude, and Longitude. This page also displays the state of the antenna in the **Antenna Connection** field as

- Unknown—Shown for early CMM2s.
- OK—Shown for later CMM2s where no problem is detected in the signal.
- Overcurrent—Indicates a coax cable or connector problem, or a problem with the unit
- Undercurrent—Indicates a coax cable or connector problem, or a problem with the unit

This information may be helpful in a decision of whether to climb a tower to diagnose a perceived antenna problem.

Accessing PPPoE Statistics About Customer Activities (SM)

When the PPPoE feature has been enabled in the SM, the PPPoE statistics provide data about the activities of the customer.

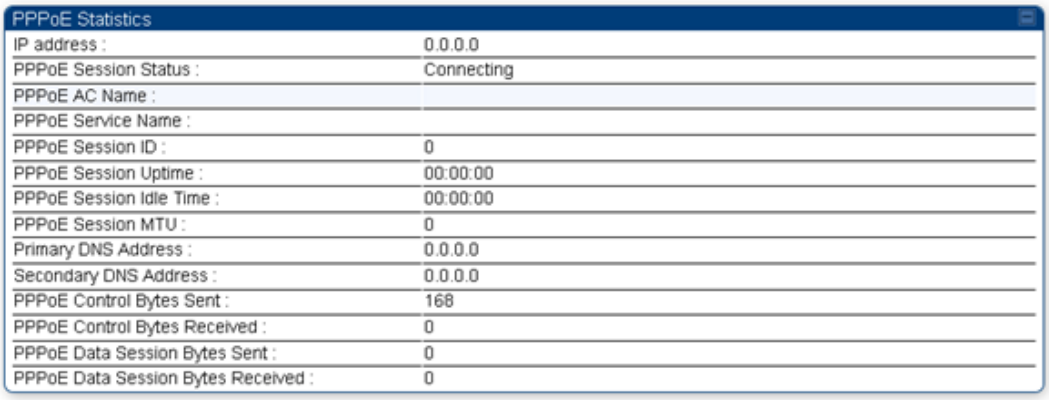

PPPoE Statistics
IP address : 0.0.0.0
PPPoE Session Status : Connecting
PPPoE AC Name :
PPPoE Service Name :
PPPoE Session ID : 0
PPPoE Session Uptime : 00:00:00
PPPoE Session Idle Time : 00:00:00
PPPoE Session MTU : 0
Primary DNS Address : 0.0.0.0
Secondary DNS Address : 0.0.0.0
PPPoE Control Bytes Sent : 168
PPPoE Control Bytes Received : 0
PPPoE Data Session Bytes Sent : 0
PPPoE Data Session Bytes Received : 0

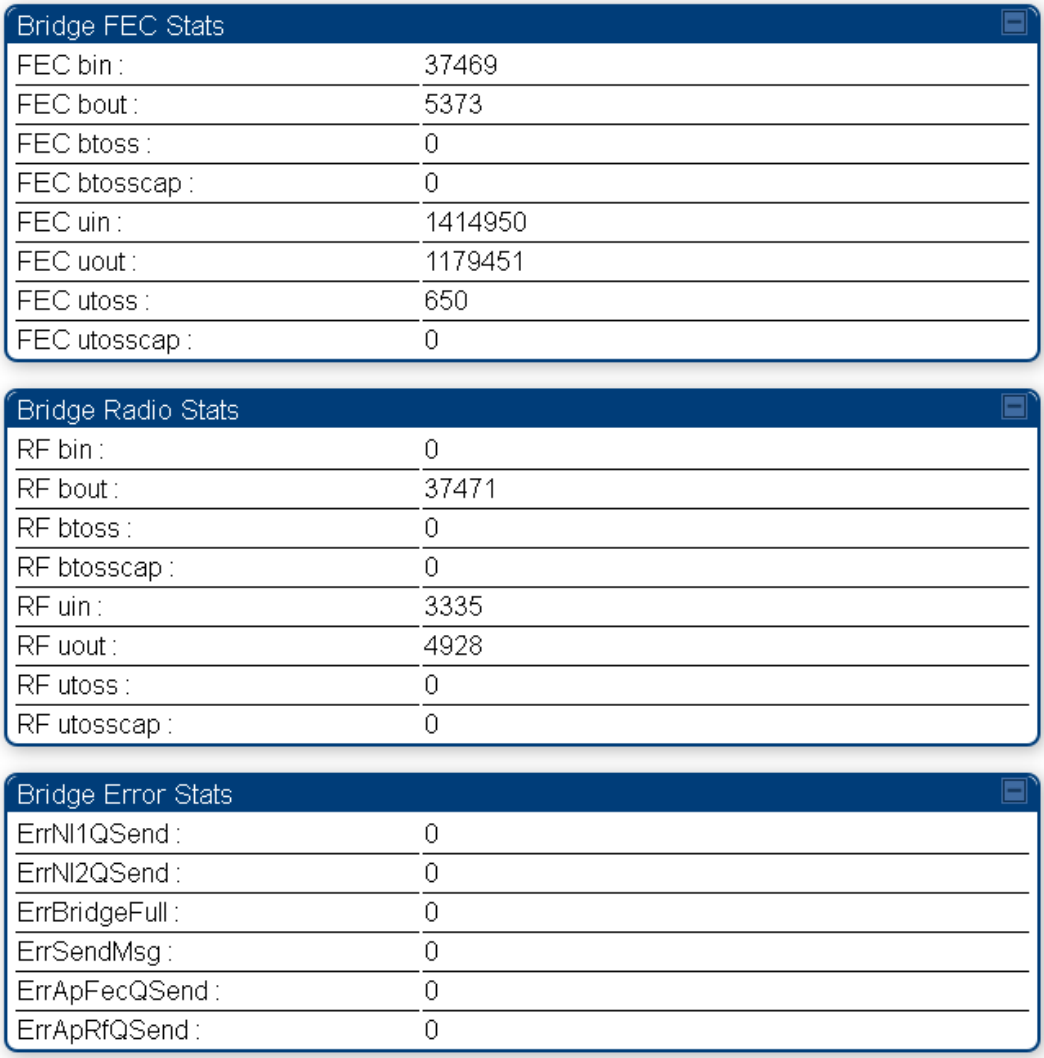
Figure 176: PPPoE tab of the SM

Attribute	Meaning
IP address	This field displays the IP address of the PPPoE session initiator (situated below the SM)
PPPoE Session Status	This field displays the operational status of the PPPoE Session
PPPoE AC Name	This field displays the access concentrator name used in the PPPoE session
PPPoE Service Name	This field displays the PPPoE service name associated with the PPPoE server in use
PPPoE Session ID	This field displays the current PPPoE session ID
PPPoE Session Uptime	This field displays the total session uptime for the PPPoE session
PPPoE Session Idle Time	This field displays the total idle time for the PPPoE session
PPPoE Session MTU	This field displays the Maximum Transmission Unit configured for the PPPoE session

Attribute	Meaning
Primary DNS Address	This field displays the primary DNS server used by the PPPoE session
Secondary DNS Address	This field displays the secondary DNS server used by the PPPoE session
PPPoE Control Bytes Sent	This field displays the total number of PPPoE session control bytes sent from the SM
PPPoE Control Bytes Received	This field displays the total number of PPPoE session control bytes received by the SM
PPPoE Data Session Bytes Sent	This field displays the total number of PPPoE data session (non-control/non-session management user data) sent by the SM
PPPoE Data Session Bytes Received	This field displays the total number of PPPoE data session (non-control/non-session management user data)

Viewing Bridge Control Block Statistics (All)

The AP and SM Bridge Control Block Statistics tab is shown below:



Bridge FEC Stats	
FEC bin :	37469
FEC bout :	5373
FEC btoss :	0
FEC btosscap :	0
FEC uin :	1414950
FEC uout :	1179451
FEC utoss :	650
FEC utosscap :	0

Bridge Radio Stats	
RF bin :	0
RF bout :	37471
RF btoss :	0
RF btosscap :	0
RF uin :	3335
RF uout :	4928
RF utoss :	0
RF utosscap :	0

Bridge Error Stats	
ErrNl1QSend :	0
ErrNl2QSend :	0
ErrBridgeFull :	0
ErrSendMsg :	0
ErrApFecQSend :	0
ErrApRfQSend :	0

Figure 177: Bridge Control Block statistics

Attribute	Meaning
FEC bin	This field indicates the number of broadcast packets received by the bridge control block on the Ethernet interface

Attribute	Meaning
FEC bout	This field indicates the number of broadcast packets sent by the bridge control block on the Ethernet interface
FEC btoss	This field indicates the number of broadcast packets tossed out by the bridge control block on the Ethernet interface
FEC btosscap	This field indicates the number of broadcast packets tossed out at the Ethernet interface due to MIR cap being exceeded.
FEC uin	This field indicates the number of unicast packets received by the bridge control block on the Ethernet interface
FEC uout	This field indicates the number of unicast packets sent by the bridge control block on the Ethernet interface
FEC utoss	This field indicates the number of unicast packets tossed by the bridge control block on the Ethernet interface
FEC utosscap	This field indicates the number of unicast packets tossed out at the Ethernet interface due to MIR cap being exceeded.
RF bin	This field indicates the number of broadcast packets received by the bridge control block on the radio interface
RF bout	This field indicates the number of broadcast packets sent by the bridge control block on the radio interface
RF btoss	This field indicates the number of broadcast packets tossed by the bridge control block on the radio interface
RF btosscap	This field indicates the number of broadcast packets tossed out at the radio interface due to MIR cap being exceeded.
RF uin	This field indicates the number of unicast packets received by the bridge control block on the radio interface
RF uout	This field indicates the number of unicast packets sent by the bridge control block on the radio interface
RF utoss	This field indicates the number of unicast packets tossed by the bridge control block on the radio interface
RF utosscap	This field indicates the number of unicast packets tossed out at the radio interface due to MIR cap being exceeded.
ErrNI1QSend	This field indicates that a packet which was sourced from the radio network stack interface 1 (Ethernet interface) could not be sent because the radio bridge queue was full. The packet was tossed out.

Attribute	Meaning
ErrNI2QSend	This field indicates that a packet which was sourced from the radio network stack interface 2 (RF interface) could not be sent because the radio bridge queue was full. The packet was tossed out.
ErrBridgeFull	This field indicates the total number of times the bridging table was full and could not accept new entries
ErrApFecQSend	This field indicates that a packet which was received on the Ethernet interface could not be processed because the radio bridge queue was full. The packet was tossed out.
ErrApRfQSend	This field indicates that a packet which was received on the RF interface could not be processed because the radio bridge queue was full. The packet was tossed out.

Chapter 28: Using Tools in the GUI

Using the Spectrum Analyzer Tool (SM, BHS)

See Monitoring the RF Environment on Page 420.

169.254.1.2

Using the Alignment Tool (SM, BHS)

An example of the Alignment Tool tab in an SM or BHS is displayed in Figure 178.

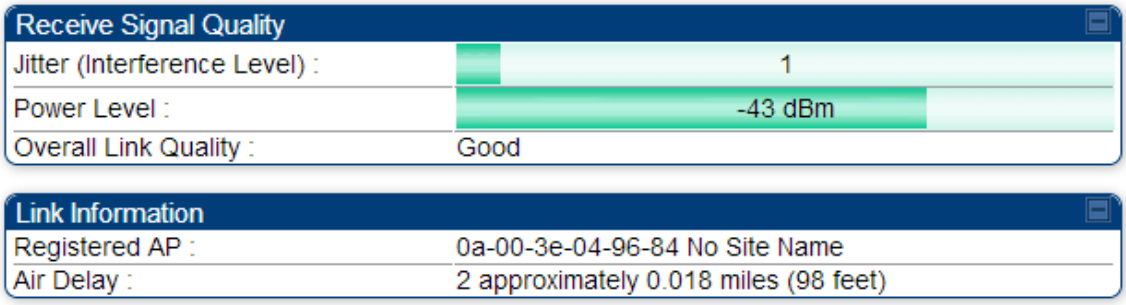


Figure 178: Alignment Tool tab of SM, example for a good link

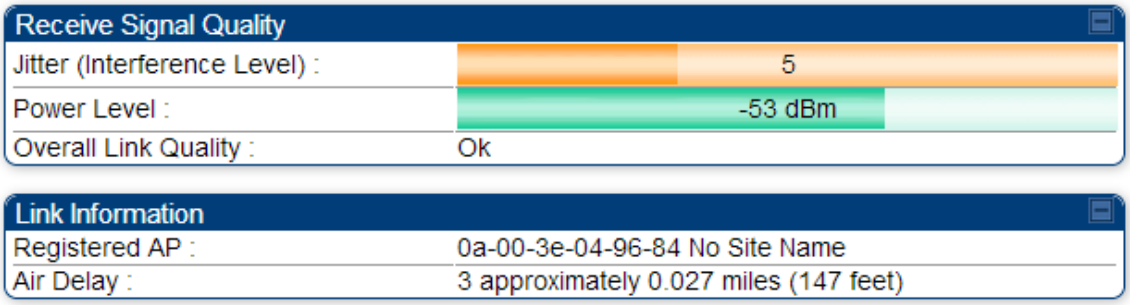


Figure 179: Alignment Tool tab of SM, example for an acceptable link

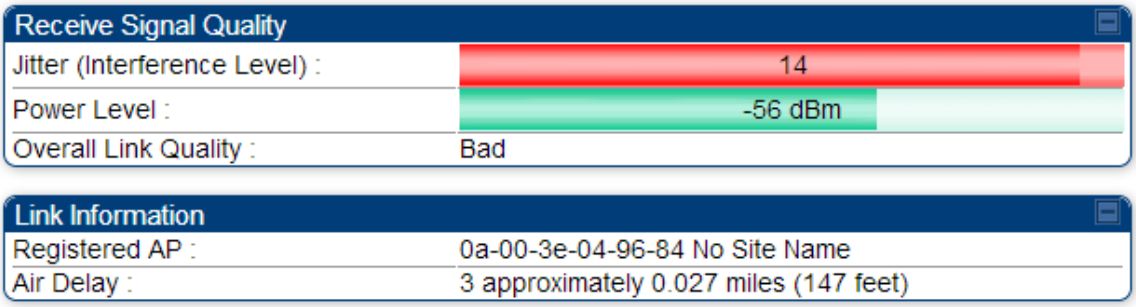


Figure 180: Alignment Tool tab of SM, example for an unacceptable link

Proper alignment must achieve all of the following indications for an acceptable link between the modules:

- power level of not less than -75dBm
- jitter value between 0 and 4
- uplink and downlink efficiency greater than 90%, except as described under Comparing Efficiency in 1X Operation to Efficiency in 2X Operation on Page 133.

IMPORTANT!
If any of these values is not achieved, a link can be established but will manifest occasional problems.

The relationship between Air Delay and link quality is described under AP-SM Links on Page 99.

Using the Link Capacity Test Tool (All)

An example of the Link Capacity Test tab is displayed in Figure 181.

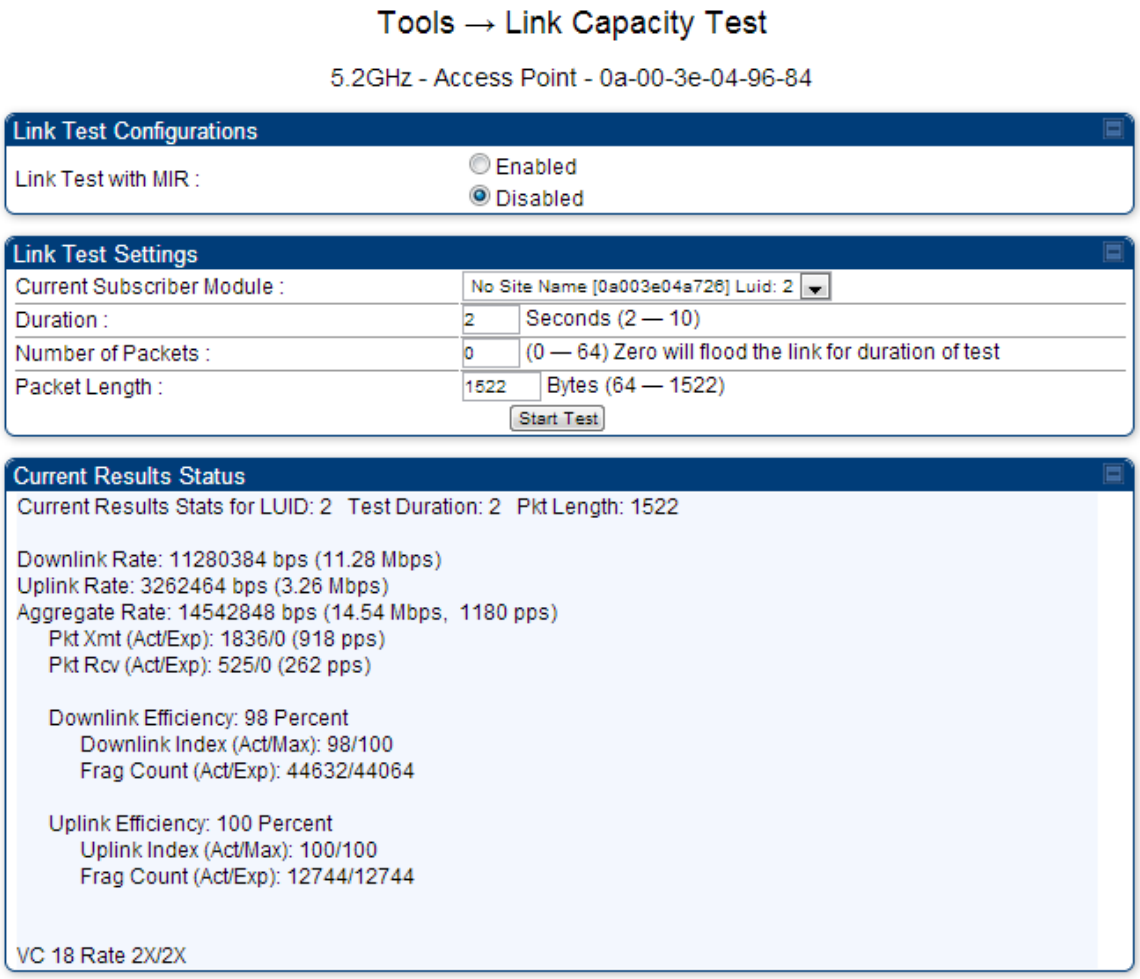

Tools → Link Capacity Test
5.2GHz - Access Point - 0a-00-3e-04-96-84
Link Test Configurations
Link Test with MIR :
Enabled
Disabled
Link Test Settings
Current Subscriber Module :
No Site Name [0a003e04a726] Luid: 2
Duration :
2
Seconds (2 — 10)
Number of Packets :
0
(0 — 64) Zero will flood the link for duration of test
Packet Length :
1522
Bytes (64 — 1522)
Start Test
Current Results Status
Current Results Stats for LUID: 2 Test Duration: 2 Pkt Length: 1522
Downlink Rate: 11280384 bps (11.28 Mbps)
Uplink Rate: 3262464 bps (3.26 Mbps)
Aggregate Rate: 14542848 bps (14.54 Mbps, 1180 pps)
Pkt Xmt (Act/Exp): 1836/0 (918 pps)
Pkt Rcv (Act/Exp): 525/0 (262 pps)
Downlink Efficiency: 98 Percent
Downlink Index (Act/Max): 98/100
Frag Count (Act/Exp): 44632/44064
Uplink Efficiency: 100 Percent
Uplink Index (Act/Max): 100/100
Frag Count (Act/Exp): 12744/12744
VC 18 Rate 2X/2X

Figure 181: Link Capacity Test tab of AP, example

The Link Capacity Test page allows you to measure the throughput and efficiency of the RF link between two modules. Many factors, including packet length, affect throughput. The Link Capacity Test tab contains the settable parameter **Packet Length** with a range of 64 to 1522 bytes. This allows you to compare throughput levels that result from various packet sizes.

For example, the same link was measured in the same time frame at a packet length of 64 bytes. The results are shown in Figure 182.

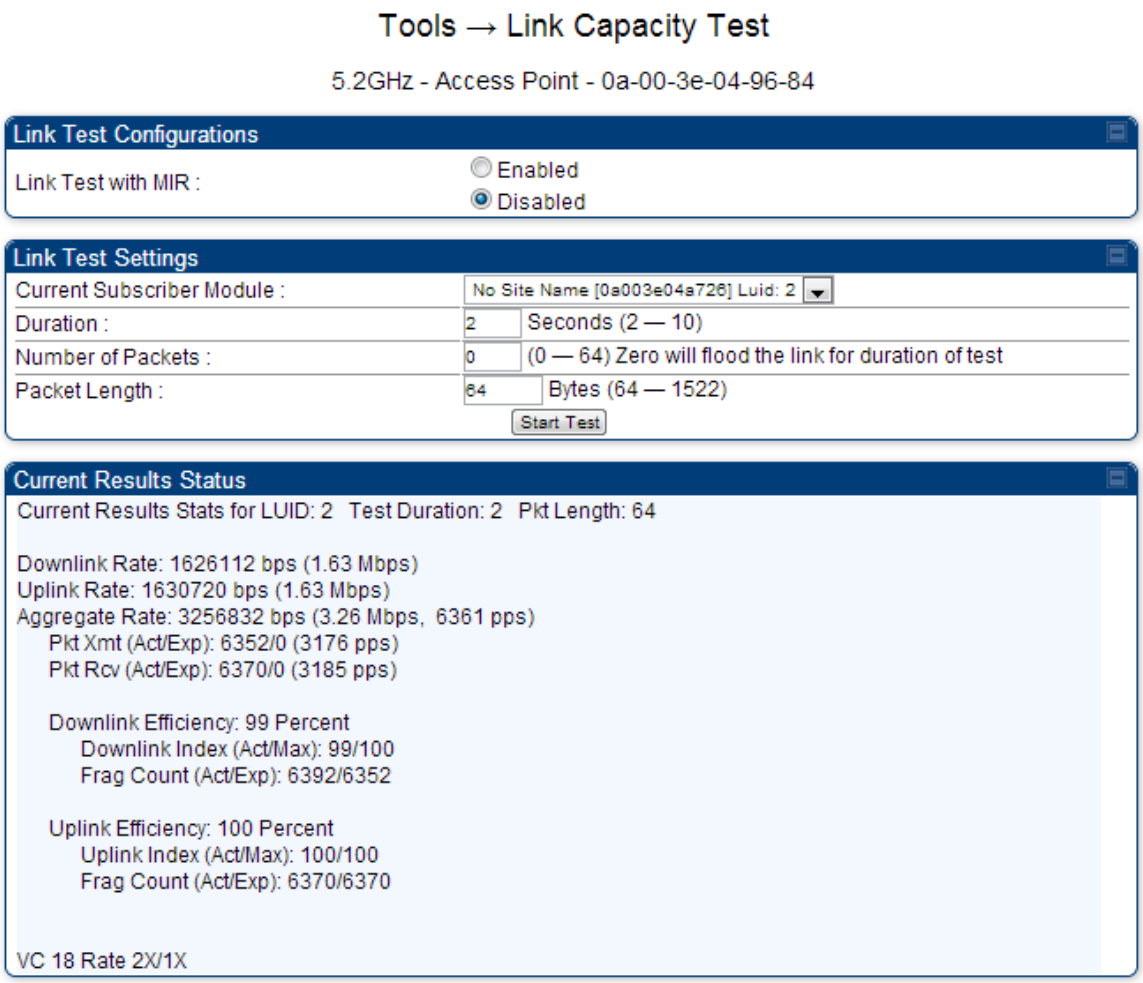

Tools → Link Capacity Test
5.2GHz - Access Point - 0a-00-3e-04-96-84
Link Test Configurations
Link Test with MIR :
Enabled
Disabled
Link Test Settings
Current Subscriber Module :
No Site Name [0a003e04a726] Luid: 2
Duration :
2
Seconds (2 — 10)
Number of Packets :
0
(0 — 64) Zero will flood the link for duration of test
Packet Length :
64
Bytes (64 — 1522)
Start Test
Current Results Status
Current Results Stats for LUID: 2 Test Duration: 2 Pkt Length: 64
Downlink Rate: 1626112 bps (1.63 Mbps)
Uplink Rate: 1630720 bps (1.63 Mbps)
Aggregate Rate: 3256832 bps (3.26 Mbps, 6361 pps)
Pkt Xmt (Act/Exp): 6352/0 (3176 pps)
Pkt Rcv (Act/Exp): 6370/0 (3185 pps)
Downlink Efficiency: 99 Percent
Downlink Index (Act/Max): 99/100
Frag Count (Act/Exp): 6392/6352
Uplink Efficiency: 100 Percent
Uplink Index (Act/Max): 100/100
Frag Count (Act/Exp): 6370/6370
VC 18 Rate 2X/1X

Figure 182: Link Capacity Test tab with 64-byte packet length, example

To test a link, perform the following steps.

Procedure 37: Performing a Link Capacity Test

1. Access the Link Capacity Test tab in the Tools web page of the module.
2. If you are running this test from an AP
   a. and you want to see Maximum Information Rate (MIR) data for the SM whose link you will be testing, then perform the following steps:
      (1) For **Link Test with MIR**, select **Enabled**.
      (2) Click the **Save Changes** button.
      (3) Click the **Reboot** button.
      (4) Similarly, set the **Link Test with MIR** parameter in the SM to **Enabled**.
      NOTE: If this parameter is enabled on one end of the link and disabled on the other, the results are misleading.
   b. use the drop-down list to select the SM whose link you want to test.
3. Type into the **Duration** field how long (in seconds) the RF link should be tested.

4. Type into the **Packet Length** field the packet length at which you want the test conducted.
5. Type into the **Number of Packets** field either
   - the number of packets (1 to 64) for the test.
   - **0** to flood the link for as long as the test is in progress.
6. Click the **Start Test** button.
7. In the Current Results Status block of this tab, view the results of the test.
8. Optionally
   a. change the packet length.
   b. repeat Steps 5 and 6.
   c. compare the results to those of other tests.
9. If you are finished with the link tests, and if you had **Link Test with MIR** enabled on both ends, disable it on both ends.
   NOTE: This safeguards against leaving it enabled on one and not the other.

The key fields in the test results are

- **Downlink RATE** and **Uplink RATE**, expressed in bits per second
- **Downlink Efficiency** and **Uplink Efficiency**, expressed as a percentage

A link is acceptable only if the efficiencies of the link test are greater than 90% in both the uplink and downlink direction, except during 2X or 3X operation. See Using Link Efficiency to Check FSK Received Signal Quality on Page 132. Whenever you install a new link, execute a link test to ensure that the efficiencies are within recommended guidelines.

The AP downlink data percentage, slot settings, other traffic in the sector, and the quality of the RF environment all affect throughput. However, a Maximum Information Rate (MIR) throttle or cap on the SM does not affect throughput.

Using the AP Evaluation or BHM Evaluation Tool (SM, BHS)

The AP Evaluation tab in the Tools web page of the SM provides information about the AP that the SM sees. Similarly, the BHM Evaluation tab of the BHS provides information about the BHM. An example of the AP Evaluation tab is shown in Figure 183.

NOTE:
The data for this page can be suppressed by the **SM Display of AP Evaluation Data** selection in the Security tab of the Configuration page in the AP.

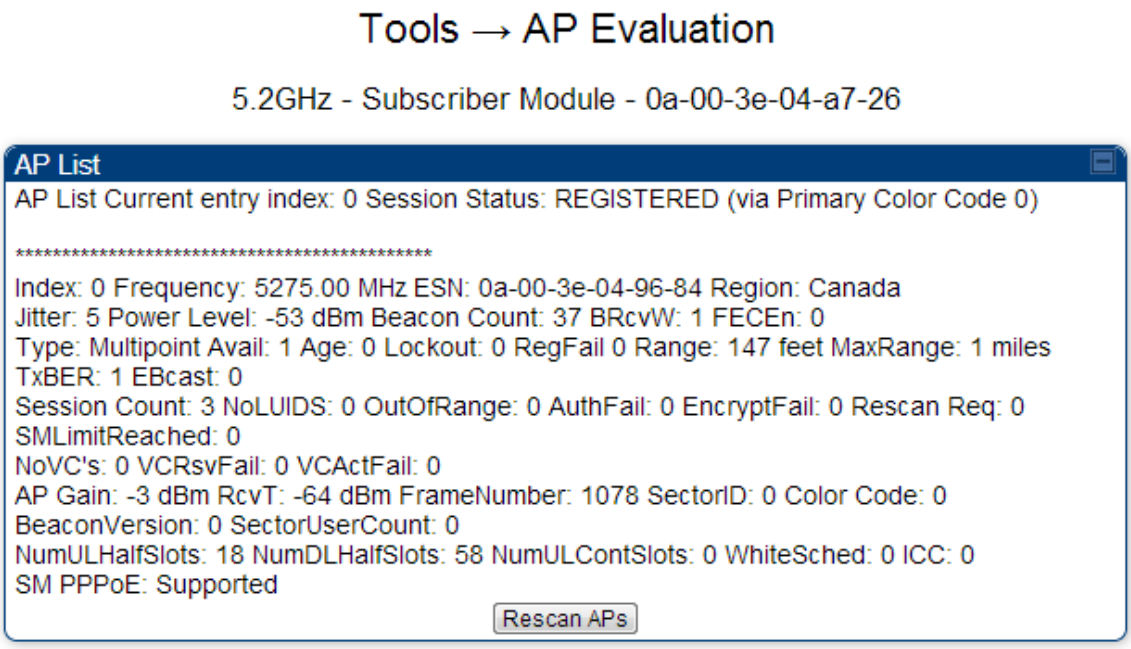

Tools → AP Evaluation
5.2GHz - Subscriber Module - 0a-00-3e-04-a7-26
AP List
AP List Current entry index: 0 Session Status: REGISTERED (via Primary Color Code 0)
****
Index: 0 Frequency: 5275.00 MHz ESN: 0a-00-3e-04-96-84 Region: Canada
Jitter: 5 Power Level: -53 dBm Beacon Count: 37 BRcvW: 1 FECEn: 0
Type: Multipoint Avail: 1 Age: 0 Lockout: 0 RegFail 0 Range: 147 feet MaxRange: 1 miles
TxBER: 1 EBcast: 0
Session Count: 3 NoLUIDS: 0 OutOfRange: 0 AuthFail: 0 EncryptFail: 0 Rescan Req: 0
SMLimitReached: 0
NoVC's: 0 VCRsvFail: 0 VCActFail: 0
AP Gain: -3 dBm RcvT: -64 dBm FrameNumber: 1078 SectorID: 0 Color Code: 0
BeaconVersion: 0 SectorUserCount: 0
NumULHalfSlots: 18 NumDLHalfSlots: 58 NumULContSlots: 0 WhiteSched: 0 ICC: 0
SM PPPoE: Supported
Rescan APs

Figure 183: AP Evaluation tab of SM, example

The AP Evaluation tab provides the following fields that can be useful to manage and troubleshoot a system:

Index

This field displays the index value that the system assigns (for only this page) to the AP where this SM is registered (or to the BHM to which this BHS is registered).

Frequency

This field displays the frequency that the AP or BHM transmits.

ESN

This field displays the MAC address (electronic serial number) of the AP or BHM. For operator convenience during SM or BHS aiming, this tab retains each detected ESN for up to 15 minutes. If the broadcast frequency of a detected AP or BHM changes during a 15-minute interval in the aiming operation, then a multiple instance of the same ESN is possible in the list. Eventually, the earlier instance expires and disappears, and the later instance remains to the end of its interval, but you can ignore the early instance(s) whenever two or more are present.

Region

Where the DFS feature is enabled, the following information follows the ESN:

- Region Code name
- Region Code numeric value
- corresponding Country Code numeric value

These are shown in the following line:

Index: 0 Frequency: 5560.00 MHz ESN: 0a-00-3e-51-60-23 Europe (RC: 3 CC: 1)

Jitter, RSSI, and Power Level

The AP Evaluation tab shows the received **Power Level** in dBm and **Jitter**. Proper alignment maximizes **Power Level** and minimizes **Jitter**. As you refine alignment, you should favor lower jitter over higher dBm. For example, if coarse alignment gives an SM a power level of −75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to −78 dBm and the jitter to 2 or 3, use the refined alignment, with the following caveats:

- When the receiving link is operating at 1X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 4.
- When the receiving link is operating at 2X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 9.

OFDM modules do not have this parameter. For historical relevance, the AP Evaluation tab also shows the **RSSI**, the unitless measure of power. Use **Power Level** and ignore **RSSI**. **RSSI** implies more accuracy and precision than is inherent in its measurement.

NOTE:
Unless the page is set to auto-refresh, the values displayed are from the instant the General Status tab was selected. To keep a current view of the values, refresh the browser screen or set to auto-refresh.

Beacon Count

A count of the beacons seen in a given time period.

BRcvW

This parameter indicates if the AP is operating with a “Big Receive Window”. A value of “1” indicates that an AP is capable of opening its receive window during the Max Range Delay section of the frame. A value of “0” indicates that the AP is capable of opening its “receive windiw” after the Max Range Delay section of the frame. This information is required so that an SM is able to transmit a registration request in the proper part of the frame.

FEC

This field contains the SNMP value from the AP that indicates whether the Forward Error Correction feature is enabled. PMP 400 Series OFDM APs do not have this field.

Type

Multipoint indicates an AP, not a BHM.

Age

This is a counter for the number of minutes that the AP has been inactive. At 15 minutes of inactivity for the AP, this field is removed from the AP Eval tab in the SM.

Lockout

This field displays how many times the SM or BHS has been temporarily locked out of making registration attempts.

RegFail

This field displays how many registration attempts by this SM or BHS failed.

Range

This field displays the distance in feet for this link. To derive the distance in meters, multiply the value of this parameter by 0.3048.

MaxRange

This field displays the AP's configured Max Range value.

TxBER

A 1 in this field indicates the AP or BHM is sending Radio BER.

EBcast

A 1 in this field indicates the AP or BHM is encrypting broadcast packets. A 0 indicates it is not.

Session Count

This field displays how many sessions the SM (or BHS) has had with the AP (or BHM). Typically, this is the sum of Reg Count and Re-Reg Count. However, the result of internal calculation may display here as a value that slightly differs from the sum.

In the case of a multipoint link, if the number of sessions is significantly greater than the number for other SMs, then this may indicate a link problem or an interference problem.

NoLUIDs

This field indicates how many times the AP has needed to reject a registration request from an SM because its capacity to make LUID assignments is full. This then locks the SM out of making any valid attempt for the next 15 minutes. It is extremely unlikely that a non-zero number would be displayed here.

OutOfRange

This field indicates how many times the AP has rejected a registration request from an SM because the SM is a further distance away than the range that is currently configured in the AP. This then locks the SM out of making any valid attempt for the next 15 minutes.

AuthFail

This field displays how many times authentication attempts from this SM have failed in the AP.

EncryptFail

This field displays how many times an encryption mismatch has occurred between the SM and the AP.

Rescan Req

This field displays how many times a re-range request has occurred for the BHM that is being evaluated in the AP Eval page of a BHS.

SMLimitReached

This field displays 0 if additional SMs may be registered to the AP. If a 1 is displayed, the AP will not accept additional SM registrations.

NoVC's

This counter is incremented when the SM is registering to an AP which determines that no VC resources are available for allocation. This could be a primary data VC or a high priority data VC.

VCRsvFail

This counter is incremented when the SM is registering to an AP which has a VC resource available for allocation but cannot reserve the resource for allocation.

VCActFail

This counter is incremented when the SM is registering to an AP which has a VC resource available for allocation and has reserved the VC, but cannot activate the resource for allocation.

AP Gain

This field displays the total external gain (antenna) used by the AP.

RcvT

This field displays the AP's configured receive target for receiving SM transmissions (this field affects automatic SM power adjust).

FrameNumber

This field displays the number from the tag applied by the FPGA to the last previous beacon frame. After the SM registers and is put into session with the AP, the value of this field is no longer kept up to date.

Sector ID

This field displays the value of the **Sector ID** field that is provisioned for the AP or BHM.

Color Code

This field displays the value of the **Color Code** field that is provisioned for the AP or BHM.

BeaconVersion

This field indicates whether the beacon is OFDM (value of 0) or FSK (value of 1).

Sector User Count

This field displays how many SMs are registered on the AP.

Frequency

This field displays the frequency of the received signal, expressed in MHz.

NumULHalfSlots

This is the number of uplink half slots in the frame for this AP or BHM. To find the number of slots, divide by 2.

NumDLHalfSlots

This is the number of downlink half slots in the frame for this AP or BHM. To find the number of slots, divide by 2.

NumULContSlots

This field displays how many control slots are being used in the uplink portion of the frame.

The AP Evaluation tab also provides the following buttons.

WhiteSched

This field numerically indicates whether the **Schedule Whitening** feature is enabled. See Schedule Whitening on Page 250. OFDM modules do not have this field.

ICC

This field displays a value of 1 when the listed AP is configured with Installation Color Code Enabled. A value of 0 is displayed when the listed AP is configured with Installation Color Code Disabled.

SM PPPoE

This field indicates whether or not an AP supports SM PPPoE sessions. APs and SMs running System Release 9.0 or greater support PPPoE sessions.

PtoP VLAN

This field indicates whether VLAN is supported in the backhaul module.

Rescan *APs or BHM*

You can click this button to force the SM or BHS to rescan the frequencies that are selected in the Radio tab of the Configuration page. (See Custom Radio Frequency Scan Selection List on Page 295.) This module will then register to the AP or BHM that provides the best results for power level, jitter, and—in an SM—the number of registered SMs.

Update Display

You can click this button to gather updated data without causing the SM or BHS to rescan and re-register.

Using the Frame Calculator Tool (All) for Co-location

The first step to avoid interference is to set all APs to receive timing from CMMs. This ensuring they are in sync and start transmitting at the same time each frame.

The second step to avoid interference is to configure parameters on all APs of the same frequency band in proximity such that they have compatible transmit/receive ratios (all stop transmitting each frame before any start receiving). This avoids the problem of one AP attempting to receive the signal from a distant SM while a nearby AP transmits, which could overpower that signal.

The following parameters on the AP determine the transmit/receive ratio:

- Max Range
- Downlink Data percentage
- (reserved) Control Slots

If all the APs of a given frequency band are FSK APs or all are OFDM APs, the simplest way to avoid interference is to set these three parameters with identical values on all APs in proximity. If OFDM and FSK APs of the same frequency band are in proximity, or if you want APs set to different parameters (differing in their Max Range values, for example), then you should use the Frame Calculator to identify compatible settings.

The frame calculator is available on the Frame Calculator tab of the Tools web page. To use the Frame Calculator, type into the calculator various configurable parameter values for each proximal AP, and then record the resulting **Uplink Rcv SQ Start** value. Next vary the **Downlink Data** percentage in each calculation and iterate until the calculated **Uplink Rcv SQ Start** for all co-located APs are within 300 bit times; if possible, within 150 bit times. In Cambium Point-to-Multipoint systems, 10 bit times = 1 μs.

OFDM modules provide an OFDM Frame Calculator and FSK modules provide an FSK Frame Calculator. To perform frame calculations for co-located OFDM and FSK modules, you must use an OFDM module for the OFDM calculations and an FSK module for the FSK calculations.

The calculator *does not* use values in the module or populate its parameters. It is merely a convenience application that runs on a module. For this reason, you can use any FSK module (AP, SM, BHM, BHS) to perform FSK frame calculations for setting the parameters on an FSK AP and any OFDM module (AP, SM, BHM, BHS) to perform OFDM frame calculations for setting the parameters on an OFDM AP.

IMPORTANT!

APs that have slightly mismatched transmit-to-receive ratios and low levels of data traffic may see little effect on throughput. A system that was not tuned for co-location may work fine at low traffic levels, but encounter problems at higher traffic levels. The conservative practice is to tune for co-location before traffic ultimately increases. This prevents problems that occur as sectors are built.

An example of the Frame Calculator tab is shown in Figure 184.

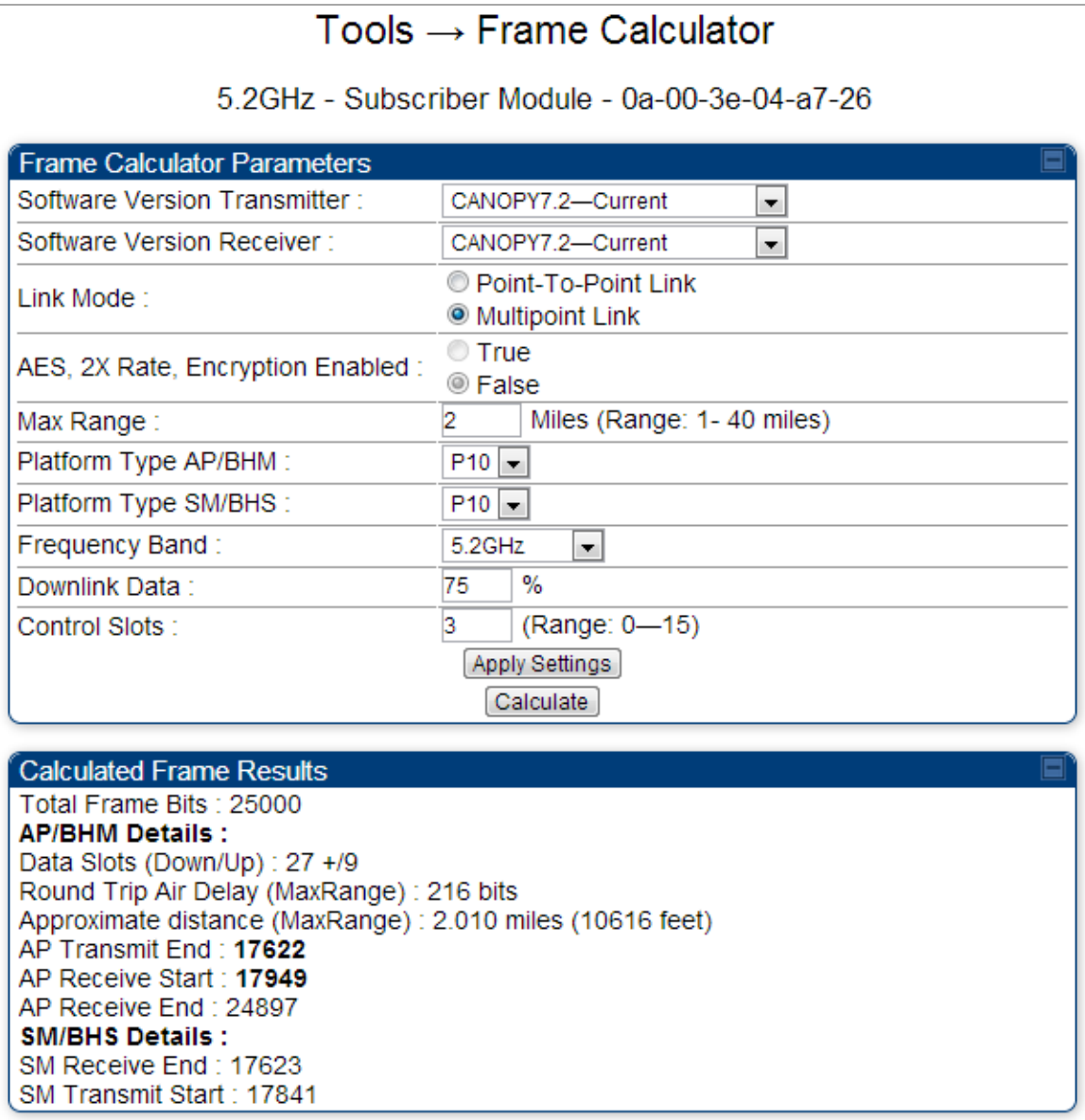


Figure 184: Frame Calculator tab, example

In the Frame Calculator tab, you may set the following parameters.

Software Version Transmitter

From the drop-down menu, select the software release that runs on the AP(s).

Software Version Receiver

From the drop-down menu, select the software release that runs on the SM(s).

Transmit Sync Input

If the APs in the cluster

- receive sync from a CMMmicro or CMM4, select **Sync to Received Signal (Power Port)**.
- receive sync from a CMM2, select **Sync to Received Signal (Timing Port)**.
- are self timed, select **Generate Sync Signal**.

Link Mode

For AP to SM frame calculations, select **Multipoint Link**.

AES, 2X Rate, Encryption Enabled

This value is not settable by the operator.

Max Range

Set to the same value as the **Max Range** parameter is set in the AP(s).

Platform Type Transmitter

Use the drop-down list to select the hardware series (board type) of the AP.

Platform Type Receiver

Use the drop-down list to select the hardware series (board type) of the SM.

Frequency Band

Use the drop-down list to select the radio frequency band of the AP and SM.

Downlink Data

Initially set this parameter to the same value that the AP has for its **Downlink Data** parameter (percentage). Then, as you use the Frame Calculator tool in Procedure 38, you will vary the value in this parameter to find the proper value to write into the **Downlink Data** parameter of all APs in the cluster.

PMP 100 Series APs offer a range of 1% to 99%, and default to 75%. PMP 400 Series APs offer a range of 1% to 90%, and default to 75%. The value that you set in this parameter has the following interaction with the value of the **Max Range** parameter (above):

- The default **Max Range** value is 5 miles and, at that distance, the maximum **Downlink Data** value (90% in OFDM) is functional.
- Where **Max Range** is set to 6 to 10 miles, **Downlink Data** should be set to not greater than 85%. This lesser maximum avoids registration problems for nearby SMs. The user interface of the OFDM AP automatically imposes the lesser maximum.

Control Slots

Set this parameter to the value of the **Control Slot** parameter is set in the APs. Since control slots are half the size of data slots, they are sometimes called half slots. **Control Slots** in the Configuration > Radio tab or Home > General Status tab of the AP are the same as **Control Half Slots** in the Tools > Frame Calculator tab.

The Calculated Frame Results display several items of interest.

To use the Frame Calculator, perform the following steps.

Procedure 38: Using the Frame Calculator

1. Use a module of the technology type (FSK or OFDM) of the first AP.
2. Populate the FSK or OFDM Frame Calculator parameters with appropriate values as described above.
3. Click the **Apply Settings** button.
4. Click the **Calculate** button.
5. Scroll down the tab to the Calculated Frame Results section.
   NOTE: An example of the Calculated Frame Results section is displayed in Figure 185.

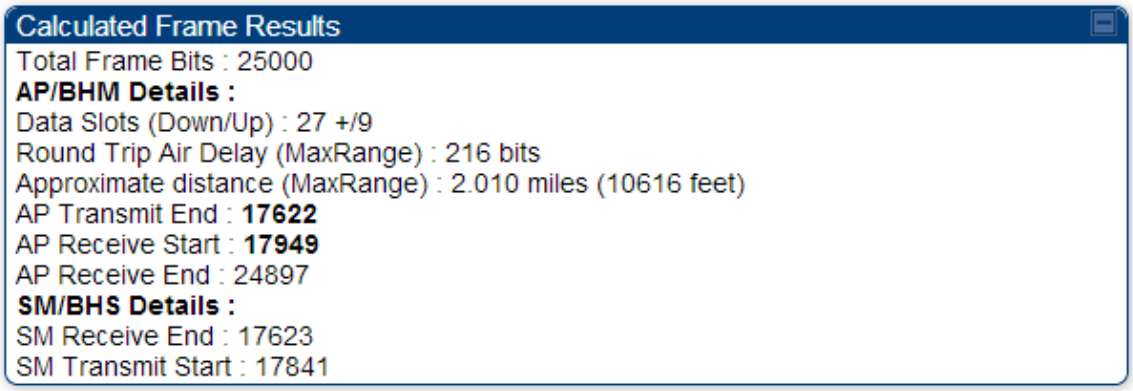

Calculated Frame Results
Total Frame Bits : 25000
AP/BHM Details :
Data Slots (Down/Up) : 27 +/9
Round Trip Air Delay (MaxRange) : 216 bits
Approximate distance (MaxRange) : 2.010 miles (10616 feet)
AP Transmit End : 17622
AP Receive Start : 17949
AP Receive End : 24897
SM/BHS Details :
SM Receive End : 17623
SM Transmit Start : 17841

Figure 185: Calculated Frame Results section of Frame Calculator tab, example

6. Record the value of the **Uplink Rcv SQ Start** field.
7. Enter a parameter set from another AP or use a different module (OFDM or FSK) to calculate results for that technology type.
8. Click the **Apply Settings** button.
9. Click the **Calculate** button.
10. Scroll down the tab to the Calculated Frame Results section. If “Invalid Configuration” is displayed, check and change values and settings, with special attention to the **Platform Type** parameters (P7, P8, and so on).
11. Record the value of the **Uplink Rcv SQ Start** field.
12. If the recorded values of the **Uplink Rcv SQ Start** field are within 150 time bits of each other, skip the next step.

13. Repeat this procedure, changing the value of the **Downlink Data** parameter until the values that this tool calculates for the **Uplink Rcv SQ Start** field are within 300 time bits of each other; if possible, within 150 time bits.
14. Access the Radio tab in the Configuration web page of each AP in the cluster and change its **Downlink Data** parameter (percentage) to the last value that you used in the Frame Calculator.

Viewing the DFS Status Tab (All)

Examples of the DFS Status tab in the Tools page are shown in Figure 186.

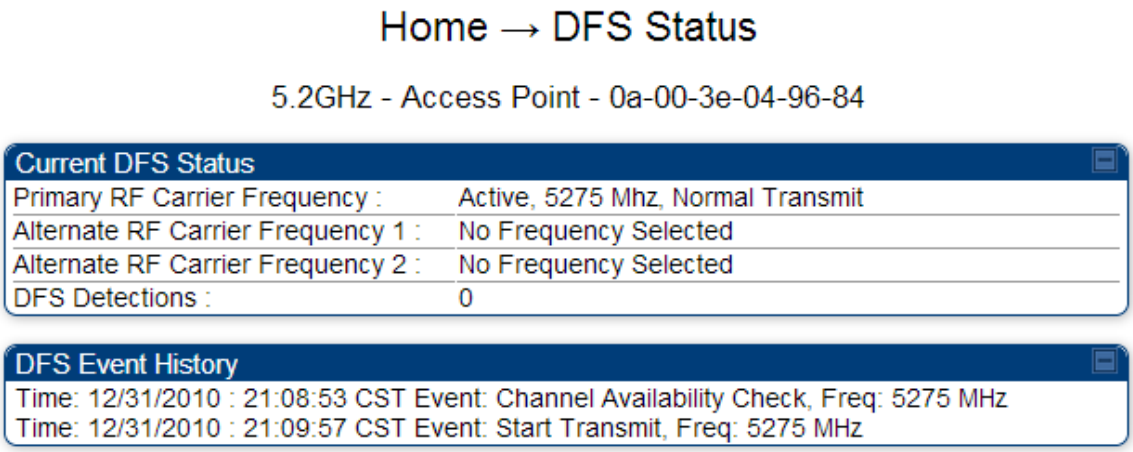

Home → DFS Status
5.2GHz - Access Point - 0a-00-3e-04-96-84
Current DFS Status
Primary RF Carrier Frequency : Active, 5275 Mhz, Normal Transmit
Alternate RF Carrier Frequency 1 : No Frequency Selected
Alternate RF Carrier Frequency 2 : No Frequency Selected
DFS Detections : 0
DFS Event History
Time: 12/31/2010 : 21:08:53 CST Event: Channel Availability Check, Freq: 5275 MHz
Time: 12/31/2010 : 21:09:57 CST Event: Start Transmit, Freq: 5275 MHz

Figure 186: DFS Status tab of AP, example

This tab provides an instant view of the current frequency in use and thus whether the Dynamic Frequency Selection (DFS) feature has shut down operation on the primary frequency to avoid competition with radar that is protected by regulation.

DFS Event History

This log is useful for seeing when DFS events happened, including the response of any **Alternate RF Carriers** that were assigned.

In the example shown in Figure 186, the AP

1. performed a 60-second Channel Availability Check (CAC).
2. started transmitting at 1:03 (mm:ss) on 5580 MHz, the Primary RF Carrier Frequency.
3. experienced a DFS hit at 6:58:58 (hh:mm:ss).
4. switched to the Alternate RF Carrier Frequency 1 (5590 MHz).
5. performed a 60-second Channel Availability Check (CAC).

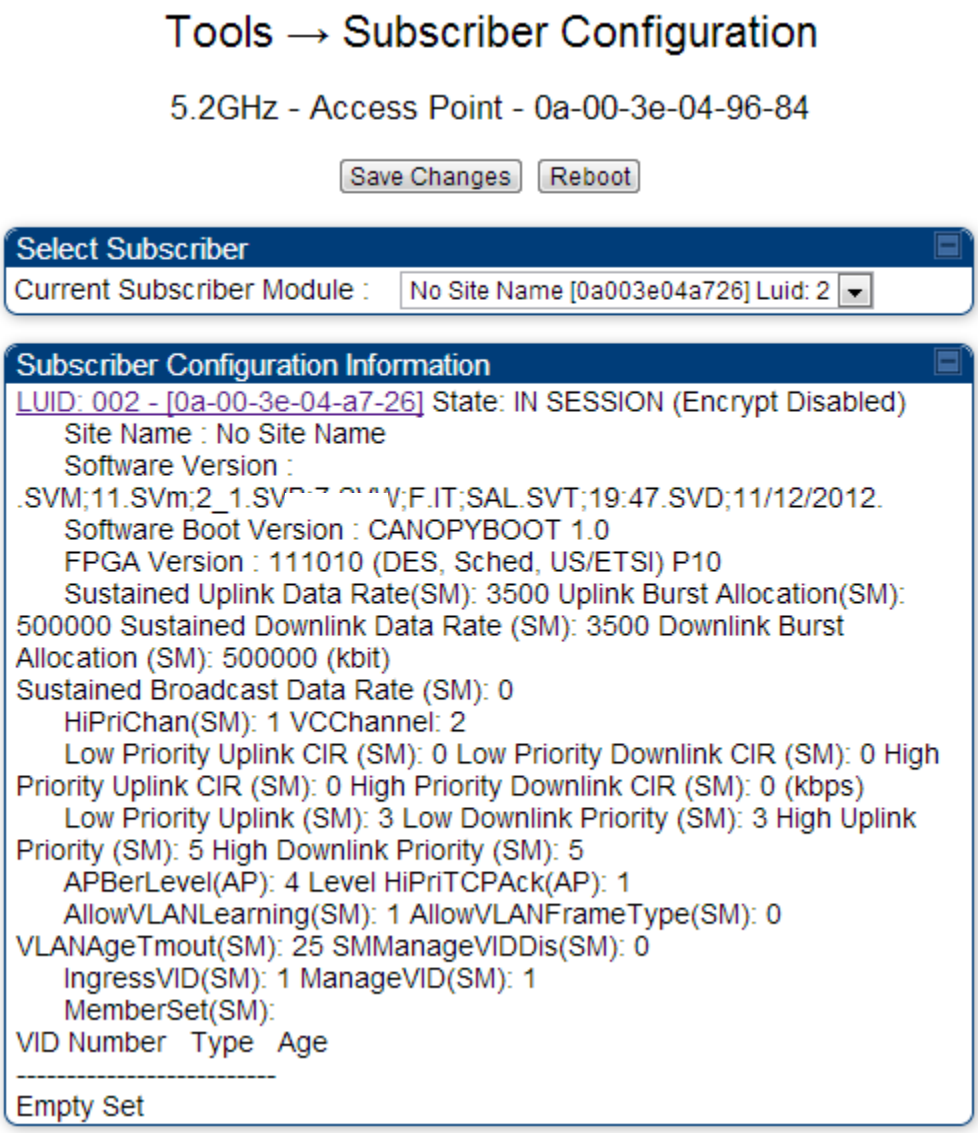
6. started transmitting on 5590 MHz.

Using the SM Configuration Tool (AP, BHM)

The SM Configuration tab in the Tools page of the AP or BHM displays

- the current values whose control may be subject to the setting in the **Configuration Source** parameter.
- an indicator of the configuration source for each value.
  - (SM) – QoS/VLAN parameters are derived from the SM's settings
  - (APCAP) – QoS/VLAN parameters are derived from the AP's settings, including any keyed capping (for radios capped at 4 Mbps, 10 Mbps, or 20 Mbps)
  - (D) – QoS/VLAN parameters are retrieved from the device, due to failed retrieval from the AAA or WM server.
  - (AAA) – QoS/VLAN parameters are retrieved from the RADIUS server
  - (BAM) – QoS/VLAN parameters are retrieved from a WM BAM server

An example of the SM Configuration tab is displayed in Figure 187.


Tools → Subscriber Configuration
5.2GHz - Access Point - 0a-00-3e-04-96-84
Save Changes
Reboot
Select Subscriber
Current Subscriber Module :
No Site Name [0a003e04a726] Luid: 2
Subscriber Configuration Information
LUID: 002 - [0a-00-3e-04-a7-26] State: IN SESSION (Encrypt Disabled)
Site Name : No Site Name
Software Version :
.SVM;11.SVm;2_1.SV
V;F.IT;SAL.SVT;19:47.SVD;11/12/2012.
Software Boot Version : CANOPYBOOT 1.0
FPGA Version : 111010 (DES, Sched, US/ETSI) P10
Sustained Uplink Data Rate(SM): 3500 Uplink Burst Allocation(SM): 500000 Sustained Downlink Data Rate (SM): 3500 Downlink Burst Allocation (SM): 500000 (kbit)
Sustained Broadcast Data Rate (SM): 0
HiPriChan(SM): 1 VCChannel: 2
Low Priority Uplink CIR (SM): 0 Low Priority Downlink CIR (SM): 0 High Priority Uplink CIR (SM): 0 High Priority Downlink CIR (SM): 0 (kbps)
Low Priority Uplink (SM): 3 Low Downlink Priority (SM): 3 High Uplink Priority (SM): 5 High Downlink Priority (SM): 5
APBerLevel(AP): 4 Level HiPriTCPAck(AP): 1
AllowVLANLearning(SM): 1 AllowVLANFrameType(SM): 0
VLANAgeTmout(SM): 25 SMManageVIDDis(SM): 0
IngressVID(SM): 1 ManageVID(SM): 1
MemberSet(SM):
VID Number Type Age

Empty Set

Figure 187: SM Configuration tab of AP, example

Indicators for configuration source are explained under Session Status Tab of the AP on Page 200.

Reviewing the Link Status Tool Results (AP)

An example of the Link Status tool results is shown in Figure 188.

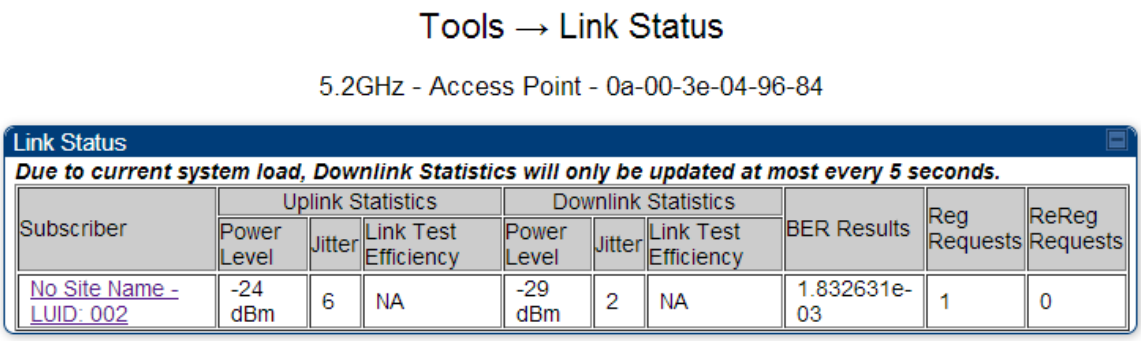


Figure 188: Link Status tab of AP, example

The Link Status tool results include values for the following fields.

Power Level
Jitter

These are reported near-instantaneously, if web refresh rate is set to 1 or 2 seconds. These values are the same as those that are displayed on the Session Status tab of the Home page in the AP and the General Status tab of the Home page in the SM.

Last Link Test Efficiency Percentage

This field displays the results of the last link test initiated from the SM. Link tests initiated from the AP *are not* shown. A link test exercises both uplink and downlink, and efficiencies for both are reported.

BER Results

This field displays the over-the-air Bit Error Rates for each downlink. (The ARQ [Automatic Resend reQuest] ensures that the transport BER [the BER seen end-to-end through a network] is essentially zero.) The level of acceptable over-the-air BER varies, based on operating requirements, but a reasonable value for a good link is a BER of 1e-4 (1×10^{-4}) or better, approximately a packet resend rate of 5%.

BER is generated using unused bits in the downlink. During periods of peak load, BER data is not updated as often, because the system puts priority on transport rather than on BER calculation.

Registration Requests
Re-registration Requests

These request counts are shown for each SM since the time of the last AP reboot. A **Registration Requests** count is the number of times the SM registered after the AP determined that the link had been down. A **Re-registration Requests** count is the number of times the AP received an SM registration request while the AP considered the link to be still up (and therefore did not expect registration requests).

Using the Remote Spectrum Analyzer Tool (AP)

The Remote Spectrum Analyzer tool in the AP provides additional flexibility in the use of the spectrum analyzer in the SM. Opearators may configure a duration of 10 to 1000 seconds and select an SM from the drop-down list, then click the **Start Remote Spectrum Analysis** button to launch the analysis from that SM. An example of this tool in the AP is shown in Figure 189.

Tools → Remote Spectrum Analyzer
5.2GHz - Access Point - 0a-00-3e-04-96-84
Access Point Stats
Registered SM Count : 1
Maximum Count of Registered SMs : 1
Configuration
Current Subscriber Module : No Site Name [0a003e04a726] Luid: 2
Duration : 10 Seconds (10—1000)
Start Remote Spectrum Analysis
Remote Results
Results retrieved successfully.
Remote Spectrum Analysis complete for 10 seconds
Display: Averaging Receiver Channel Bandwidth: 20.0 MHz
System time at start of analysis: 21:27:45 12/31/2010 CST
Site Name: No Site Name Location: No Site Location Contact: No Site Contact
Freq |-100 |-95 |-90 |-85 |-80 |-75 |-70 |-65 |-60 |-55 |-50 |-45 |-40 dBm Inst Avg Max
Data : SpectrumAnalysis.xml
Green bars indicate the average signal strength per frequency over the duration of the scan
Yellow bars indicate maximum received signal strength per frequency over the duration of the scan
Red bars indicate received signal strength greater than -40 dBm over the duration of the scan

Figure 189: Remote Spectrum Analyzer tab of AP, example

This feature proceeds in the following sequence:

1. The AP de-registers the target SM.
2. The SM scans (for the duration set in the AP tool) to collect data for the bar graph.
3. The SM re-registers to the AP.
4. The AP displays the bar graph.

The bar graph is an HTML file, but can be changed to an XML file, which is then easy to analyze through the use of scripts that you may write for parsing the data. To transform the file to XML, click the SpectrumAnalysis.xml link. Although the resulting display appears mostly unchanged, the bar graph is now coded in XML. You can now right-click on the bar graph for a **Save Target As** option to save the `Spectrum Analysis.xml` file.

Using the BER Results Tool (SM, BHS)

Radio BER data represents bit errors at the RF link level. Due to CRC checks on fragments and packets and ARQ (Automatic Repeat reQuest), the BER of customer data is essentially zero. Radio BER gives one indication of link quality. Other important indications to consider include the received power level, jitter, and link tests. Radio BER is supported on FSK and OFDM radios.

BER is only instrumented on the downlink and is displayed on the BER Results tab of the Tools page in any SM. Each time the tab is clicked, the current results are read, and counters are reset to zero. An example of the BER Results tab is displayed in Figure 190.

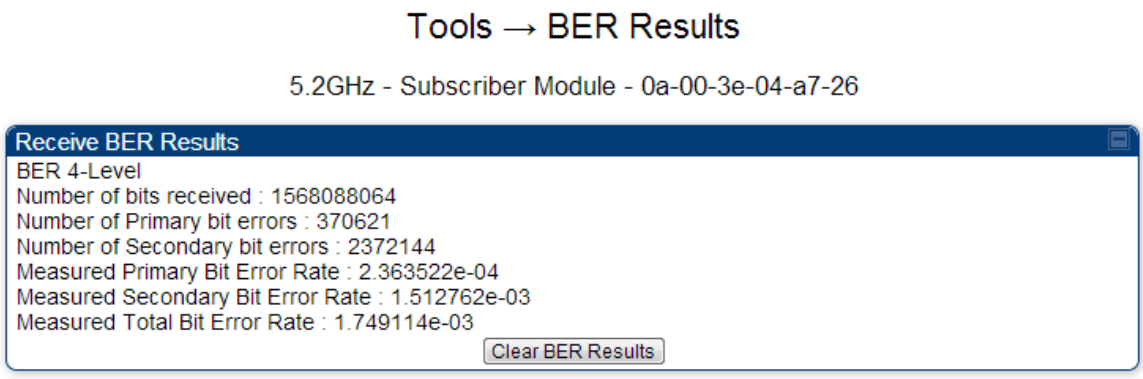

Tools → BER Results
5.2GHz - Subscriber Module - 0a-00-3e-04-a7-26
Receive BER Results
BER 4-Level
Number of bits received : 1568088064
Number of Primary bit errors : 370621
Number of Secondary bit errors : 2372144
Measured Primary Bit Error Rate : 2.363522e-04
Measured Secondary Bit Error Rate : 1.512762e-03
Measured Total Bit Error Rate : 1.749114e-03
Clear BER Results

Figure 190: BER Results tab of FSK SM, example

The BER Results tab can be helpful in troubleshooting poor link performance. The value in the **Measured Total Bit Error Rate** field represents the bit error rate (BER) in the RF link since the last time the BER Results tab was clicked. If the AP is enabled for 2X operation, then this tab displays both **Primary** (1X) and **Secondary** (2X) **Bit Error Rate** fields. If the link sometimes operates in 2X, then the **Measured Secondary Bit Error Rate** field is populated by a measurement.

The link is acceptable if the value of this field is less than 10^{-4}. If the BER is greater than 10^{-4}, re-evaluate the installation of both modules in the link.

The BER test signal is broadcast by the AP (and compared to the expected test signal by the SM) only when capacity in the sector allows it. This signal is the lowest priority for AP transmissions.

Chapter 29: Maintaining Your Software

Cambium provides release compatibility information and caveats about each release. For the latest information and caveats about each software release, see the release notes available for download from http://www.cambiumnetworks.com/support/pmp/software/index.php .

Typical Contents of Release Notes

Cambium supports each release with software release notes, which include

- description of features that are introduced in the new release.
- issues that the new release resolves.
- known issues and special notes for the new release.
- installation procedures for the new release.

Typical Upgrade Process

In a typical upgrade process, proceed as follows:

1. Visit http://www.cambiumnetworks.com/support/pmp/software/index.php .
2. Click the appropriate radio series to view supporting documennts
3. Read the compatibility information and any caveats that Cambium associates with the release.
4. Read the software release notes from the web site.
5. On the basis of these, decide whether the release is appropriate for your network.
6. Enter your name, email address, and CCN# or unit MAC Address (ESN).
7. Download the software release and associated files.
8. Use CNUT to manage the upgrade across your network.

NOTE:
After the initial 12-month standard warranty, an annual Software Maintenance Contract must be obtained to continue receiving software updates and technical support. The contract includes minor software enhancements as they become available and 24/7 telephone support. Contracts are available through Cambium's authorized reseller partners or directly from the Technical Support

Center with a credit card.

Major software feature enhancements may require the purchase of a license key and/or new hardware.

Downloading Software and Release Notes

All supported software releases, the associated software release notes document, and updated MIB files are available for download at any time from http://www.cambiumnetworks.com/support/pmp/software/index.php. This web site also typically provides a summary of the backward compatibility and any advantages or disadvantages of implementing the release.

When you click on the release that you wish to download, you are prompted for information that identifies yourself and your organization (such as name, address, and e-mail address). When you complete and submit the form that prompts for this information, the download is made available to you.

Rebranding Module Interface Screens

Distinctive fonts indicate

literal user input.
variable user input.
literal system responses.
variable system responses.

The interface screens on each module display the Canopy or Canopy Advantage logo. These logos can be replaced with other logos using Procedure 39.

The logo is a hyperlink, and clicking on it takes the user to the Canopy web site. A different site (perhaps the operator's support site) can be made the destination using Procedure 40.

To return a module to regular logos and hyperlinks, use Procedure 41.

The logo at the top of each page is a key indicator to the user whether a module is Canopy or Canopy Advantage. If you choose to replace the logos, use two noticeably different logos so that users can continue to easily distinguish between a Canopy module and a Canopy Advantage module.

To replace logos and hyperlinks efficiently throughout your network, read the following two procedures, write a script, and execute your script through the Canopy Network Updater Tool (CNUT).[9] To replace them individually, use one of the following two procedures.

Procedure 39: Replacing the Canopy logo on the GUI with another logo

1. If the current logo is the Canopy logo, name your custom logo file on your computer `canopy.jpg` and put it in your home directory.

   If the current logo is the Canopy Advantage logo, name your custom logo file on your computer `advantaged.jpg` and put it in your home directory.

2. Use an FTP (File Transfer Protocol) session to transfer this file to the module, as in the example session shown in Figure 191.

[9] See Using the Canopy Network Updater Tool (CNUT) on Page 417.

```
> ftp ModuleIPAddress
Connected to ModuleIPAddress
220 FTP server ready
Name (ModuleIPAddress:none): root
331 Guest login ok
Password: <password-if-configured>
230 Guest login ok, access restrictions apply.

ftp> binary
200 Type set to I
ftp> put canopy.jpg
OR
      put advantaged.jpg
OR
      put top.html
ftp> quit
221 Goodbye
```

Figure 191: Example ftp session to transfer custom logo file

3. Use a telnet session and the **addwebfile** command to add the new file to the file system, as in the example session shown in Figure 192.

NOTE:
Supported telnet commands execute the following results:

- **addwebfile** adds a custom logo file to the file system.
- **clearwebfile** clears the logo file from the file system.
- **lsweb** lists the custom logo file and display the storage space available on the file system.

```
>telnet ModuleIPAddress
/---------\
C A N O P Y

Cambium Networks
(Copyright 2001-2012 Cambium Networks)

Login: root
Password: <password-if-configured>

Telnet +> addwebfile canopy.jpg
    OR
          addwebfile advantaged.jpg
    OR
          addwebfile top.html

Telnet +> lsweb

Flash Web files
/canopy.jpg     7867
free directory entries: 31
free file space: 55331

Telnet +> exit
```

Figure 192: Example telnet session to activate custom logo file

Procedure 40: Changing the URL of the logo hyperlink

1. In the editor of your choice, create a file named `top.html`, consisting of one line:

   `<a href="myurl">`

   where ***myurl*** is the desired URL
2. Save and close the file as `top.html`.
3. Use an FTP (File Transfer Protocol) session to transfer this file to the module, as in the example session shown in Figure 191 on Page 558.
4. Use a telnet session and the addwebfile command to add the new file (top.html) to the file system, as in the example session shown in Figure 192.

If you ever want to restore the original logo and hyperlink in a module, perform the following steps.

Procedure 41: Returning a module to its original logo and hyperlink

1. Use a telnet session and the clearwebfile command to clear all custom files from the file system of the module, as in the example session shown in Figure 193 below.

```
>telnet ModuleIPAddress
/---------\
C A N O P Y

Cambium Networks
(Copyright 2001-2012 Cambium Networks)

Login: root
Password: <password-if-configured>

Telnet +> lsweb
Flash Web files
canopy.jpg     7867
free directory entries: 31
free file space: 56468

Telnet +> clearwebfile
Telnet +> lsweb

Flash Web files
free directory entries: 32
free file space     64336 bytes

Telnet +> exit
```

Figure 193: Example telnet session to clear custom files

Setting Up a Protocol Analyzer on Your Network

Selection of protocol analyzer software and location for a protocol analyzer depend on both the network topology and the type of traffic to capture. However, the examples in this section are based on free-of-charge Wireshark software, which is available at http://www.wireshark.com

The equipment required to set up a protocol analyzer includes:

- 1 hub

> **NOTE**
>
> Some Ethernet switches have a monitor mode (also called 'port mirroring', 'port monitoring'). To ensure that all packets are captured, set up a monitoring port on the hub/switch to monitor/mirror the ports to which the network equipment and premises are connected.

- 1 laptop computer with protocol analyzer software installed
- 2 straight-through Ethernet cables
- 1 power converter

Analyzing Traffic at an SM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the SM. If the SM has DHCP enabled, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, then ensure that the laptop computer is configured with a static IP address in the same subnet as the SM.

The configuration for analyzing traffic at an SM is shown below:

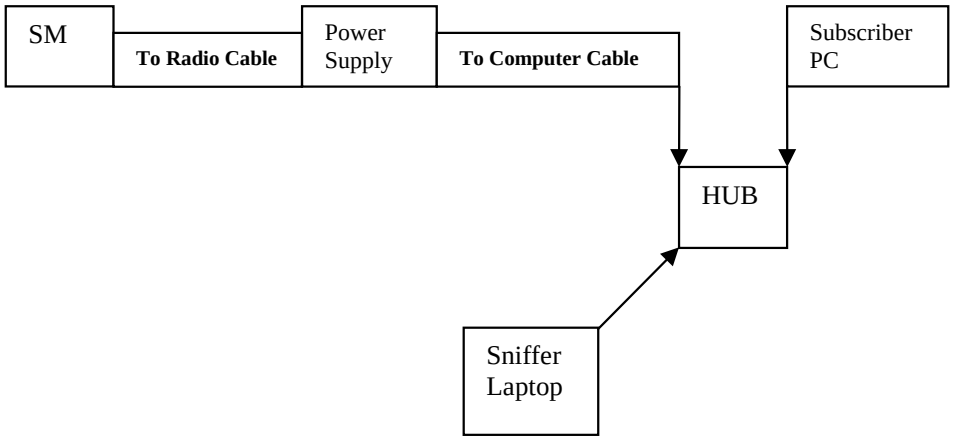


Figure 194: Protocol analysis at the SM

Analyzing traffic at an AP or BH with no CMM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the AP. If the router is configured to be a DHCP server, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, then ensure that the laptop computer is configured with a static IP address in the same subnet as the AP.

The configuration for analyzing traffic at an AP that *is not* connected to a CMM is shown below:

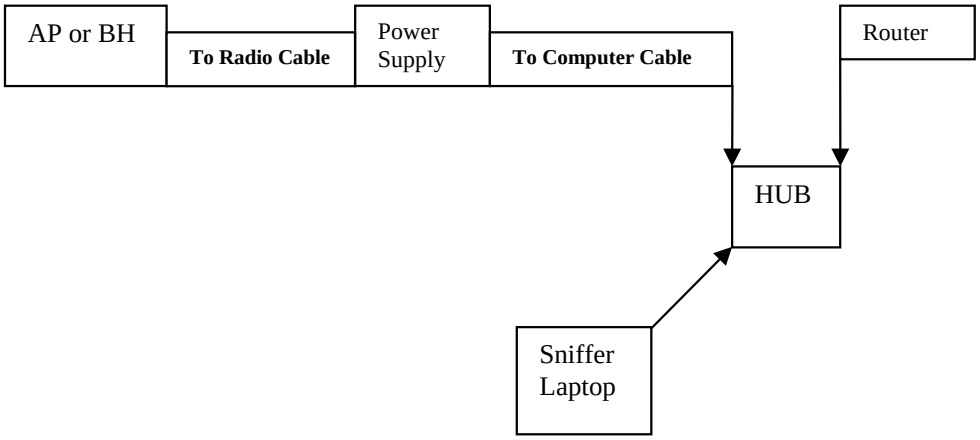


Figure 195: Protocol analyzer at AP not connected to a CMM

Analyzing Traffic at an AP or BH with a CMM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the AP. If the router is configured to be a DHCP server, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, ensure that the laptop computer is configured with a static IP address in the same subnet as the AP.

Connect the hub to the J2 Ethernet to Switch of the port that is associated with the AP. This example is of capturing traffic from AP 111, which is connected to
Port 1.

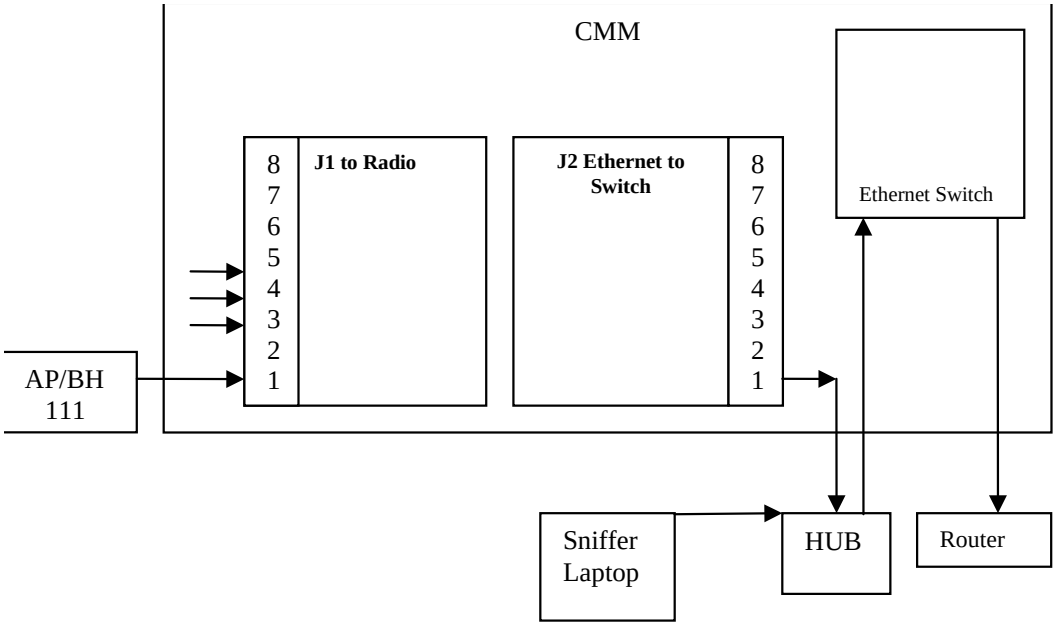


Figure 196: Protocol analysis at AP connected to a CMM

Example of a Protocol Analyzer Setup for an SM

The following is an example of a network protocol analyzer setup using Wireshark® software to capture traffic at the SM level. The Wireshark network protocol analyzer has changed its name to Wireshark™, but functionality and use remains much the same. This example is based on the following assumptions:

- All required physical cabling has been completed.
- The hub, protocol analyzer laptop computer, and subscriber PC are successfully connected.
- The SM is connected
  - as shown in Figure 194 on page 561.
  - to the subscriber PC and the AP.
- Wireshark software is operational on the laptop computer.

Although these procedures involve the SM, the only difference in the procedure for analyzing traffic on an AP or BH is the hub insertion point.

Procedure 42: Setting up a protocol analyzer

1. Note the IP configuration of the SM.
2. Browse to **Start→My Network Places→Network and Dialup Connections**.
3. For **Local Area Connection**, select **Properties**.
   RESULT: The Local Area Connections Properties window opens

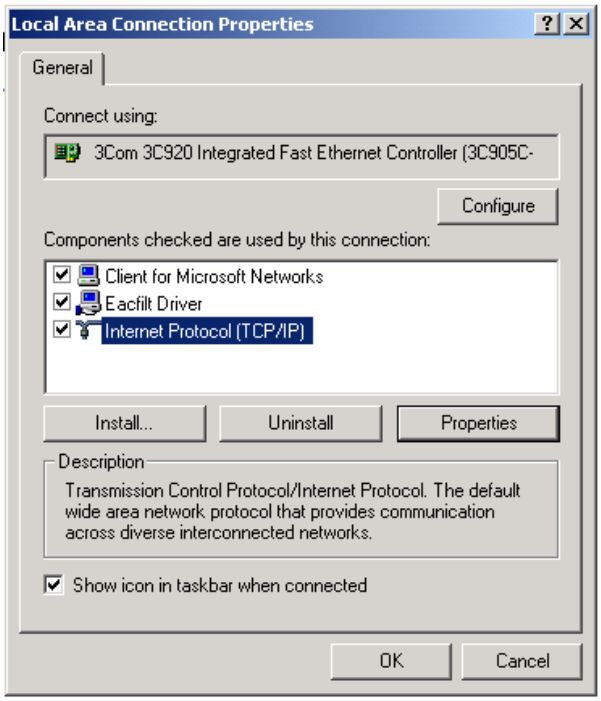


Figure 197: Local Area Connection Properties window

4. Select **Internet Protocol (TCP/IP)**.
5. Click the **Properties** button.
   RESULT: The Internet Protocol (TCP/IP) Properties window opens

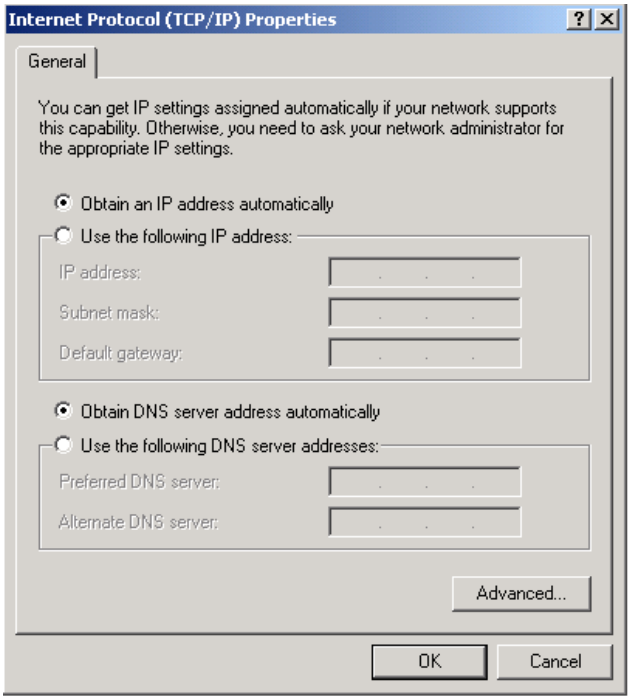

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 198: Internet Protocol (TCP/IP) Properties window

6. Unless you have a static IP address configured on the SM, select **Obtain an IP address automatically** for the protocol analyzer laptop computer. If you have configured a static IP address on the SM, then
   a. select **Use the following IP address**.
   b. enter an IP address that is in the same subnet as the SM.
7. Click **OK**.
8. Open your web browser.
9. Enter the IP address of the SM.
   RESULT: The General Status tab of the SM opens, as shown in Figure 69 on Page 207.
10. If the General Status tab did not open, reconfigure how the laptop computer obtains an IP address.
11. Verify that you have connectivity from the laptop computer to the SM with the hub inserted.
12. Launch the protocol analyzer software on the laptop computer.
13. In the **Capture** menu, select **Start**.
    RESULT: The Wireshark Capture Options window opens

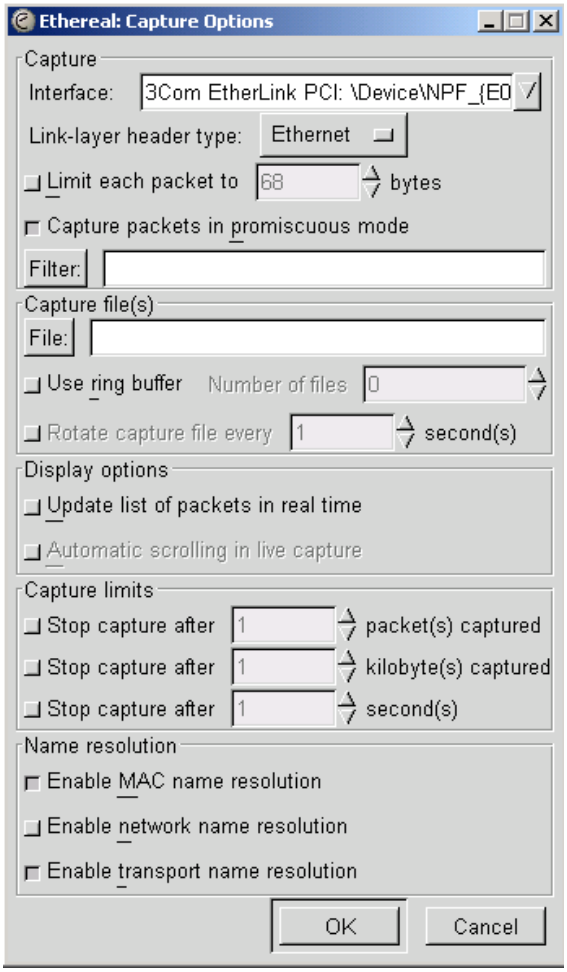


Figure 199: Wireshark Capture Options window

14. Ensure that the **Interface** field reflects the network interface card (NIC) that is used on the protocol analyzer laptop computer.
    NOTE: Although you can select filters based on specific types of traffic, all values are defaults in this example.
15. If you wish to select filters, select them now.
16. Click **OK**.
    RESULT: The Wireshark Capture window opens

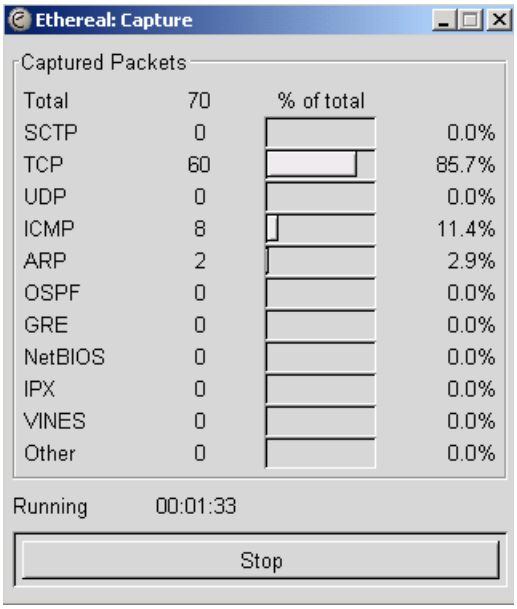


Figure 200: Wireshark Capture window

NOTE: This window graphically displays the types of packets (by percentage) that are being captured.

17. If all packet types are displayed with 0%, either
    - launch your Web browser on the subscriber PC for the IP address of the SM
    - ping the SM from the home PC.
18. If still all packet types are displayed with 0% (meaning that no traffic is being captured), reconfigure IP addressing until you can successfully see traffic captured on the laptop computer.
19. Whenever the desired number of packets have been captured, click **Stop**.
    RESULT: When you stop the packet capture, the <capture> - Wireshark window opens

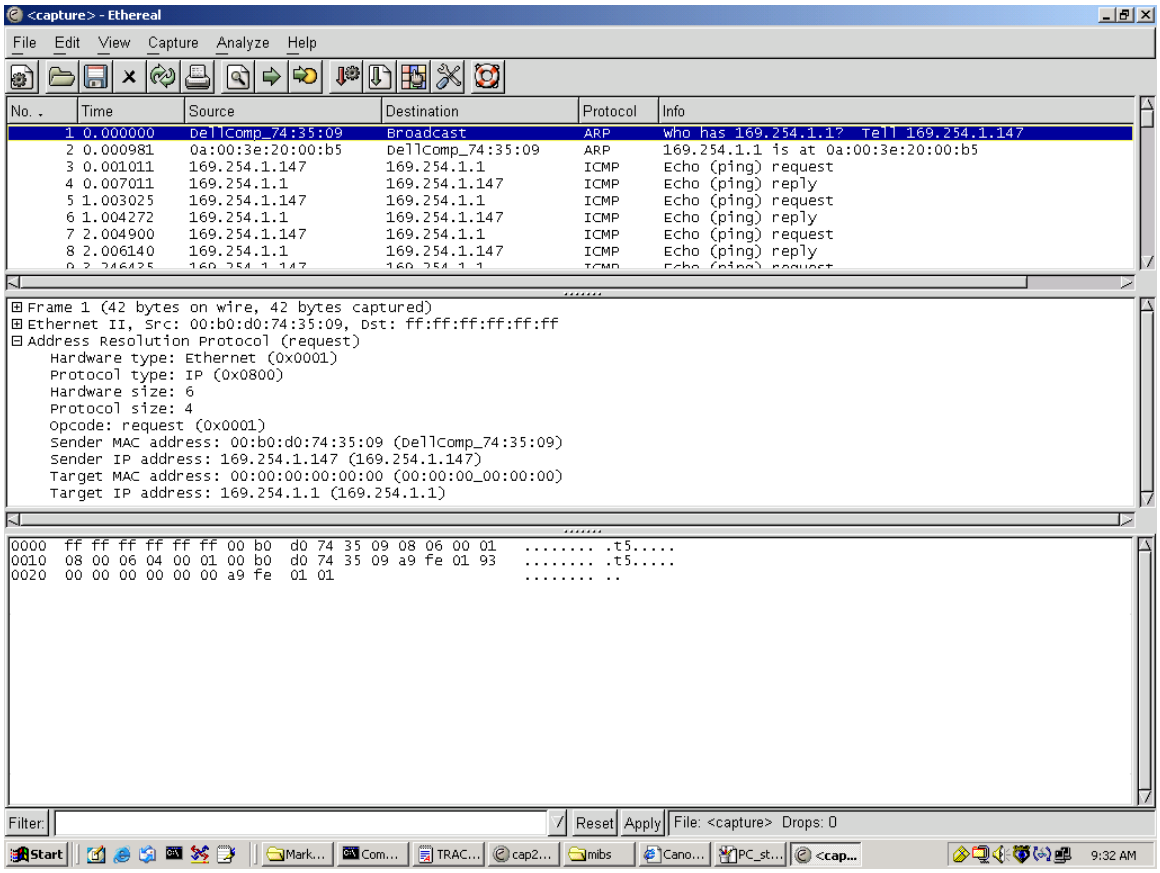

<capture> - Ethereal
File Edit View Capture Analyze Help
No. Time Source Destination Protocol Info
1 0.000000 DellComp_74:35:09 Broadcast ARP Who has 169.254.1.1? Tell 169.254.1.147
2 0.000981 0a:00:3e:20:00:b5 DellComp_74:35:09 ARP 169.254.1.1 is at 0a:00:3e:20:00:b5
3 0.001011 169.254.1.147 169.254.1.1 ICMP Echo (ping) request
4 0.007011 169.254.1.1 169.254.1.147 ICMP Echo (ping) reply
5 1.003025 169.254.1.147 169.254.1.1 ICMP Echo (ping) request
6 1.004272 169.254.1.1 169.254.1.147 ICMP Echo (ping) reply
7 2.004900 169.254.1.147 169.254.1.1 ICMP Echo (ping) request
8 2.006140 169.254.1.1 169.254.1.147 ICMP Echo (ping) reply
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:b0:d0:74:35:09, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (0x0001)
Sender MAC address: 00:b0:d0:74:35:09 (DellComp_74:35:09)
Sender IP address: 169.254.1.147 (169.254.1.147)
Target MAC address: 00:00:00:00:00:00 (00:00:00_00:00:00)
Target IP address: 169.254.1.1 (169.254.1.1)
0000 ff ff ff ff ff ff 00 b0 d0 74 35 09 08 06 00 01 ..... .t5.....
0010 08 00 06 04 00 01 00 b0 d0 74 35 09 a9 fe 01 93 ..... .t5.....
0020 00 00 00 00 00 00 a9 fe 01 01 ....
Filter: Reset Apply File: <capture> Drops: 0
Start
9:32 AM

Figure 201: <capture> - Wireshark window, Packet 1 selected

This window has three panes:

- The top pane provides a sequenced summary of the packets captured and includes SRC/DEST address and type of protocol. What you select in this pane determines the additional information that is displayed in the lower two panes.
- The lower two panes facilitate drill-down into the packet that you selected in the top pane.

In this example, Packet 1 (a broadcast ARP request) was selected in the top pane. The lower two panes provide further details about Packet 1.

Another example is shown below.

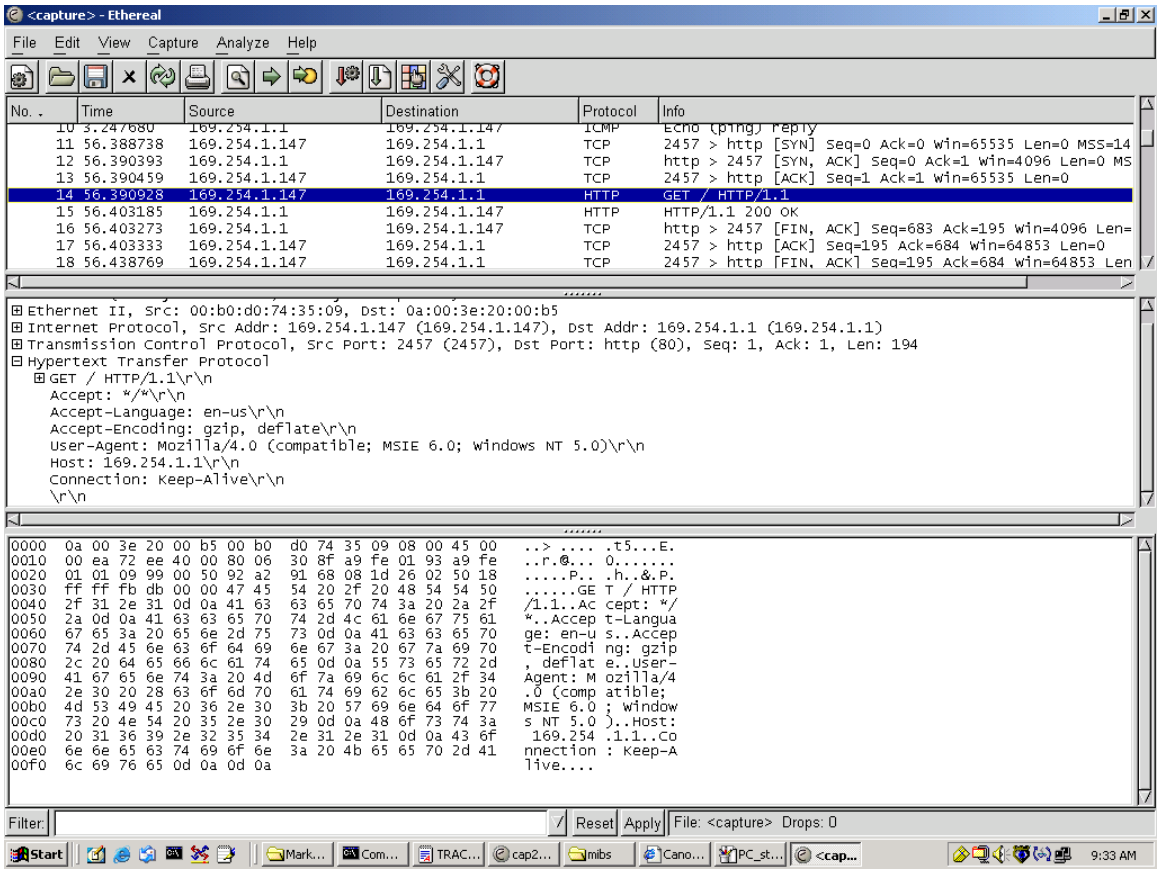


Figure 202: <capture> - Wireshark window, Packet 14 selected

In this second example, Packet 14 (protocol type HTTP) is selected in the top pane. The two lower panes provide further details about Packet 14.

Chapter 30: Troubleshooting

General Planning for Troubleshooting

Effective troubleshooting depends in part on measures that you take before you experience trouble in your network. Cambium recommends the following measures for each site:

1. Identify troubleshooting tools that are available at your site (such as a protocol analyzer).
2. Identify commands and other sources that can capture baseline data for the site. These may include
   - **`ping`**
   - **`tracert`** or **`traceroute`**
   - Link Capacity Test results
   - throughput data
   - Configuration tab captures
   - Status tab captures
   - session logs
3. Start a log for the site.
4. Include the following information in the log:
   - operating procedures
   - site-specific configuration records
   - network topology
   - software releases, boot versions, and FPGA firmware versions
   - types of hardware deployed
   - site-specific troubleshooting processes
   - escalation procedures
5. Capture baseline data into the log from the sources listed in Step 2.

General Fault Isolation Process

Effective troubleshooting also requires an effective fault isolation methodology that includes

- attempting to isolate the problem to the level of a system, subsystem, or link, such as
  - AP to SM
  - AP to CMM
  - AP to GPS
  - CMM to GPS

- BHM to BHS
- BHM to CMM
- power

- researching Event Logs of the involved equipment. (See Interpreting Messages in the Event Log on Page 504.)
- answering the questions listed in the following section.
- reversing the last previous corrective attempt before proceeding to the next.
- performing only one corrective attempt at a time.

Questions to Help Isolate the Problem

When a problem occurs, attempt to answer the following questions:

1. What is the history of the problem?
   - Have we changed something recently?
   - Have we seen other symptoms before this?
2. How wide-spread is the symptom?
   - Is the problem on only a single SM? (If so, focus on that SM.)
   - Is the problem on multiple SMs? If so
     - is the problem on one AP in the cluster? (If so, focus on that AP)
     - is the problem on multiple, but not all, APs in the cluster? (If so, focus on those APs)
     - is the problem on all APs in the cluster? (If so, focus on the CMM and the GPS signal.)
3. Based on data in the Event Log (described in Interpreting Messages in the Event Log on Page 504)
   - does the problem correlate to External Hard Resets with no WatchDog timers? (If so, this indicates a loss of power. Correct your power problem.)
   - is intermittent connectivity indicated? (If so, verify your configuration, power level, jitter, cables and connections, and the speed duplex of both ends of the link).
   - does the problem correlate to loss-of-sync events?
4. Are connections made via *shielded* cables?
5. Does the GPS antenna have an *unobstructed* view of the entire horizon?

Secondary Steps

After preliminary fault isolation through the above steps

1. check the Canopy knowledge base (http://www.cambiumnetworks.com/forum/) to find whether other network operators have encountered a similar problem.
2. proceed to any appropriate set of diagnostic steps. These are organized as follows:
   - Module Has Lost or Does Not Establish Connectivity
   - NAT/DHCP-configured SM Has Lost or Does Not Establish Connectivity on Page 573
   - SM Does Not Register to an AP on Page 574
   - BHS Does Not Register to the BHM on Page 575
   - Module Has Lost or Does Not Gain Sync on Page 576
   - Module Does Not Establish Ethernet Connectivity on Page 576
   - Module Does Not Power Up on Page 577
   - Power Supply Does Not Produce Power on Page 578
   - CMM Does Not Pass Proper GPS Sync to Connected Modules on Page 578

Procedures for Troubleshooting

Module Has Lost or Does Not Establish Connectivity

To troubleshoot a loss of connectivity, perform the following steps.

Procedure 43: Troubleshooting loss of connectivity

1. Isolate the end user/SM from peripheral equipment and variables such as routers, switches, and firewalls.
2. Set up the minimal amount of equipment.
3. On each end of the link
   a. check the cables and connections.
   b. verify that the cable/connection scheme—straight-through or crossover—is correct.
   c. verify that the LED labeled LNK is green.
   d. access the General Status tab in the Home page of the module.
   e. verify that the SM is registered.
   f. verify that RSSI is 700 or higher.
   g. verify that jitter is reported as 9 or lower.
   h. access the IP tab in the Configuration page of the module.
   i. verify that IP addresses match and are in the same subnet.
4. On the SM end of the link
   a. verify that the PC that is connected to the SM is correctly configured to obtain an IP address through DHCP.
   b. execute **`ipconfig`**.

c. verify that the PC has an assigned IP address.

5. On each end of the link
   a. access the General tab in the Configuration page of each module.
   b. verify that the setting for **Link Speeds** (or negotiation) matches that of the other module.
   c. access the Radio tab in the Configuration page of each module.
   d. verify that the **Radio Frequency Carrier** setting is checked in the Custom Radio Frequency Scan Selection List.
   e. verify that the **Color Code** setting matches that of the other module.
   f. access the browser LAN settings (for example, at **Tools→Internet Options→Connections→LAN Settings** in Internet Explorer).
   g. verify that none of the settings are selected.
   h. access the Link Capacity Test tab in the Tools page of the module.
   i. perform a link test. (See Procedure 37: Performing a Link Capacity Test on Page 535.)
   j. verify that the link test results show efficiency greater than 90% in both the uplink and downlink (except as described under Comparing Efficiency in 1X Operation to Efficiency in 2X Operation on Page 133).
   k. execute **`ping`**.
      NOTE: A ping size larger than 1494 Bytes to a module times out and fails. However, a ping of this size or larger to a system that is behind a Canopy module typically succeeds. It is generally advisable to ping such a system, since Canopy handles that ping with the same priority as is given all other transport traffic. The results are unaffected by ping size and by the load on the Canopy module that brokers this traffic.
   l. verify that no packet loss was experienced.
   m. verify that response times are not significantly greater than
      - 2.5 ms from BH to BH
      - 4 ms from AP to SM
      - 15 ms from SM to AP
   n. replace any cables that you suspect may be causing the problem.
6. After connectivity has been re-established, reinstall network elements and variables that you removed in Step 1.

NAT/DHCP-configured SM Has Lost or Does Not Establish Connectivity

Before troubleshooting this problem, identify the NAT/DHCP configuration from the following list:

- NAT with DHCP Client (**DHCP** selected as the **Connection Type** of the WAN interface) and DHCP Server
- NAT with DHCP Client (**DHCP** selected as the **Connection Type** of the WAN interface)
- NAT with DHCP Server
- NAT without DHCP

To troubleshoot a loss of connectivity for an SM configured for NAT/DHCP, perform the following steps.

Procedure 44: Troubleshooting loss of connectivity for NAT/DHCP-configured SM

1. Isolate the end user/SM from peripheral equipment and variables such as routers, switches, and firewalls.
2. Set up the minimal amount of equipment.
3. On each end of the link
   a. check the cables and connections.
   b. verify that the cable/connection scheme—straight-through or crossover—is correct.
   c. verify that the LED labeled LNK is green.
4. At the SM
   a. access the NAT Table tab in the Logs web page.
   b. verify that the correct NAT translations are listed.
   RESULT: NAT is eliminated as a possible cause if these translations are correct.
5. If this SM is configured for NAT with DHCP, then at the SM
   a. execute **`ipconfig`**.
   b. verify that the PC has an assigned IP address.
   c. if the PC *does not* have an assigned IP address, then
      - enter **`ipconfig /release “Adapter Name”`**.
      - enter **`ipconfig /renew “Adapter Name”`**.
      - reboot the PC.
      - retreat to Step 5a.

      if the PC has an assigned IP address, then
      - access the NAT DHCP Statistics tab in the Statistics web page of the SM.
      - verify that DHCP is operating as configured.
6. After connectivity has been re-established, reinstall network elements and variables that you removed in Step 1.

SM Does Not Register to an AP

To troubleshoot an SM failing to register to an AP, perform the following steps.

Procedure 45: Troubleshooting SM failing to register to an AP

1. Access the Radio tab in the Configuration page of the SM.
2. Note the **Color Code** of the SM.
3. Access the Radio tab in the Configuration page of the AP.
4. Verify that the **Color Code** of the AP matches that of the SM.
5. Note the **Radio Frequency Carrier** of the AP.
6. Verify that the value of the **RF Frequency Carrier** of the AP is selected in the **Custom Radio Frequency Scan Selection List** parameter in the SM.
7. In the AP, verify that the **Max Range** parameter is set to a distance slightly greater than the distance between the AP and the furthest SM that must register to this AP.
8. Verify that a clear line of sight exists between the AP and the SM, and that no obstruction significantly penetrates the Fresnel zone of the attempted link. If these conditions are not established, then verify that the AP and SM are 900-MHz modules in close proximity to each other.
9. Access the General Status tab in the Home page of each module.
10. In the **Software Version** field, verify that both the AP and SM are of the same encryption scheme (AES or DES).
11. Remove the bottom cover of the SM to expose the LEDs.
12. Power cycle the SM.
    RESULT: Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the SM is in Alignment mode because the SM failed to establish the link.
13. In this latter case, and if the SM has encountered no customer-inflicted damage, then request an RMA for the SM.

BHS Does Not Register to the BHM

To troubleshoot an BHS failing to register to the BHM, perform the following steps.

Procedure 46: Troubleshooting BHS failing to register to a BHM

1. Access the Radio tab in the Configuration page of the BHS.
2. Note the **Color Code** of the BHS.
3. Access the Radio tab in the Configuration page of the BHM.
4. Verify that the **Color Code** of the BHM matches that of the BHS.
5. Note the **Radio Frequency Carrier** of the BHM.
6. Verify that the value of the **RF Frequency Carrier** of the BHM is selected in the **Custom Radio Frequency Scan Selection List** parameter on the Configuration page of the BHS.
7. Verify that a clear line of sight exists between the BHM and BHS, and that no obstruction significantly penetrates the Fresnel zone of the attempted link.
8. Access the General Status tab in the Home page of each module.
9. In the **Software Version** field, verify that both the BHM and BHS are of the same encryption scheme (AES or DES).

10. Also in the **Software Version** field, verify that both the BHM and BHS are of the same modulation rate from the factory (BH20 or BH10).
11. Remove the bottom cover of the BHS to expose the LEDs.
12. Power cycle the BHS.
    RESULT: Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the BHS is in Alignment mode because the BHS failed to establish the link. In this latter case, and if the BHS has encountered no customer-inflicted damage, then request an RMA for the BHS.

Module Has Lost or Does Not Gain Sync

To troubleshoot a loss of sync, perform the following steps.

Procedure 47: Troubleshooting loss of sync

1. Access the Event Log tab in the Home page of the SM.
2. Check for messages with the following format:
   `RcvFrmNum =`
   `ExpFrmNum =`
   (See Table 74: Event Log messages for abnormal events on Page 505.)
3. If these messages are present, check the Event Log tab of another SM that is registered to the same AP for messages of the same type.
4. If the Event Log of this second SM *does not* contain these messages, then the fault is isolated to the first SM.

   If the Event Log page of this second SM contains these messages, access the GPS Status page of the AP.
5. If the **Satellites Tracked** field in the GPS Status page of the AP indicates fewer than 4 or the **Pulse Status** field does not indicate Generating Sync, check the GPS Status page of another AP in the same AP cluster for these indicators.
6. If these indicators are present in the second AP
   a. verify that the GPS antenna still has an unobstructed view of the entire horizon.
   b. visually inspect the cable and connections between the GPS antenna and the CMM.
   c. if this cable is not shielded, replace the cable with shielded cable.
7. If these indicators *are not* present in the second AP
   a. visually inspect the cable and connections between the CMM and the AP antenna.
   b. if this cable is not shielded, replace the cable with shielded cable.

Module Does Not Establish Ethernet Connectivity

To troubleshoot a loss of Ethernet connectivity, perform the following steps.

Procedure 48: Troubleshooting loss of Ethernet connectivity

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. If the Ethernet cable connects the module to a network interface card (NIC), verify that the cable is pinned out as a straight-through cable.
4. If the Ethernet cable connects the module to a hub, switch, or router, verify that the cable is pinned out as a crossover cable.
5. Verify that the Ethernet port to which the cable connects the module is set to auto-negotiate speed.
6. Power cycle the module.
   RESULT: Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the module is in Alignment mode because the module failed to establish the link.
7. In this latter case, and if the module has encountered no customer-inflicted damage, then request an RMA for the module.

Module Does Not Power Up

To troubleshoot the failure of a module to power up, perform the following steps.

Procedure 49: Troubleshooting failure to power up

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. Verify that the cable is wired and pinned out according to the specifications provided under Wiring Connectors on Page 188.
4. Remove the cover of the module to expose the components on the printed wiring board.
5. Find the Ethernet transformer, which is labeled with either the name Halo or the name Pulse.
6. Verify that the Ethernet transformer does not show damage that would have been caused by improper cabling. (You can recognize damage as the top of the transformer being no longer smooth. The transformer in the following picture is damaged and is ineligible for an RMA.)

7. Connect the power supply to a known good module via a known good Ethernet cable.
8. Attempt to power up the known good module and

- if the known good module fails to power up, request an RMA for the power supply.
- if the known good module powers up, return to the module that does not power up.

9. Reconnect the power supply to the failing module.
10. Connect the power supply to a power source.
11. Verify that the red LED labeled PWR lights.
12. If this LED *does not* light, and the module has not been powered up since the last previous FPGA firmware upgrade was performed on the module, then request an RMA for the module.

Power Supply Does Not Produce Power

To troubleshoot the failure of a power supply to produce power, perform the following steps.

Procedure 50: Troubleshooting failure of power supply to produce power

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. Verify that the cable is wired and pinned out according to the specifications provided under Wiring Connectors on Page 188.
4. Connect the power supply to a known good module via a known good Ethernet cable.
5. Attempt to power up the known good module.
6. If the known good module fails to power up, request an RMA for the power supply.

CMM Does Not Pass Proper GPS Sync to Connected Modules

If the Event Log tabs in all connected modules contain `Loss of GPS Sync Pulse` messages, perform the following steps.

Procedure 51: Troubleshooting CMM not passing sync

1. Verify that the GPS antenna has an unobstructed view of the entire horizon.
2. Verify that the GPS coaxial cable meets specifications.
3. Verify that the GPS sync cable meets specifications for wiring and length.
4. If the web pages of connected modules indicate any of the following, then find and eliminate the source of noise that is being coupled into the GPS sync cable:
   - In the GPS Status page
     - anomalous number of **Satellites Tracked** (greater than 12, for example)
     - incorrect reported **Latitude** and/or **Longitude** of the antenna
   - In the Event Log page

- garbled GPS messages
- large number of `Acquired GPS Sync Pulse` messages

5. If these efforts fail to resolve the problem, then request an RMA for the CMM.

Module Software Cannot be Upgraded

If your attempt to upgrade the software of a module fails, perform the following steps.

Procedure 52: Troubleshooting an unsuccessful software upgrade

1. Download the latest issue of the target release and the associated release notes.
2. Compare the files used in the failed attempt to the newly downloaded software.
3. Compare the procedure used in the failed attempt to the procedure in the newly downloaded release notes.
4. If these comparisons reveal a difference, retry the upgrade, this time with the newer file or newer procedure.
5. If, during attempts to upgrade the FPGA firmware, the following message is repeatable, then request an RMA for the module:

   ```
   Error code 6, unrecognized device
   ```

Module Functions Properly, Except Web Interface Became Inaccessible

If a module continues to pass traffic, and the telnet and SNMP interfaces to the module continue to function, but the web interface to the module does not display, perform the following steps.

Procedure 53: Restoring the web interface to a module

1. Enter **`telnet`** ***`DottedIPAddress`***.
   RESULT: A telnet session to the module is invoked.
2. At the `Login` prompt, enter **`root`**.
3. At the Password prompt, enter ***`PasswordIfConfigured`***.
4. At the `Telnet +>` prompt, enter **`reset`**.
   RESULT: The web interface is accessible again, and this telnet connection is closed.

Reference Information

Chapter 31: Administering Modules through Telnet Interface

The telnet administrative interface to a module supports the commands that are defined in Table 82. (Many of these are not needed with CNUT.)

Table 82: Supported telnet commands for module administration

Command	System help Definition	Notes
addwebfile	Add a custom web file	Syntax: **addwebfile *filename***. Copies the custom web file *filename* to non-volatile memory.
burnfile	Burn flash from file	Syntax: **burnfile *filename***. Updates the CPU firmware with a new image. User the image contained in *filename* if *filename* is provided. If provided, *filename* must match the module type (for example, SMboot.bin for a Subscriber Module or APboot.bin for an Access Point Module).
cat	Concatenate and display.	Syntax: **cat *filename***. Displays the contents of *filename*.
clearsyslog	Clear the system event log	Syntax: **clearsyslog**. Clears the system event log.
clearwebfile	Clear all custom web files	Syntax: **clearwebfile**. Deletes all *custom* web files.
exit	Exit from telnet session	Syntax: **exit**. Terminates the telnet interface session.
fpga_conf	Update FPGA program	Syntax: **fpga_conf**. Forces a module to perform a hard (FPGA and CPU) reset. (See reset.)
ftp	File transfer application	Syntax: **ftp**. Launches the ftp client application on the module.
help	Display command line function help	Syntax: **help**. Displays a list of available telnet commands and a brief description of each.
jbi	Update FPGA program	Syntax: **jbi –aprogram *file.jbc***. Updates the FPGA firmware with the new image contained in *file.jbc*.
ls	List the contents of a directory	Syntax: **ls**. Lists the file names of all files in the directory. Syntax: **ls –l**. Displays additional information, such as the sizes and dates of the files.

Command	System help Definition	Notes
lsweb	List Flash Web files	Syntax: **lsweb**. Lists the file names of the saved custom web files.
ping[10]	Send ICMP ECHO_REQUEST packets to network hosts	Syntax: **ping *IPaddress***. Sends an ICMP ECHO_REQUEST to *IPaddress* and waits for a response. If a response is received, the system returns *IPaddress* is alive. If no response is received, the system returns no answer from *IPaddress*.
reset	Reboot the unit	Syntax: **reset**. Forces the module to perform a hard (FPGA and CPU) module reset. (See **fpga_conf**.)
rm	Remove (unlink) files	Syntax: **rm *filename***. Remove *filename*.
syslog	Display system event log: syslog <optional filename>	Syntax: **syslog**. Displays the contents of the system log. Syntax: **syslog *filename***. Saves the contents of the system log to *filename*. Caution: overwrites *filename* if it already exists.
telnet	Telnet application	Syntax: **telnet *hostIPaddress***. Launches the telnet client application on the module.
tftp	tftp application	Syntax: **tftp *hostIPaddress***. Launches the tftp client application on the module.
update	Enable automatic SM code updating	Syntax: **update *actionlist.txt***. Enables the automated update procedure that *actionlist.txt* specifies. (Supported for only the Access Point Module.)
updateoff	Disable automatic SM code updating	Syntax: **updateoff**. Disables the automated update procedure.
version	Display the software version string	Syntax: **version**. Displays the module version string, which contains the software/firmware/hardware versions, the module type, and the operating frequency.

[10] See Module Has Lost or Does Not Establish Connectivity on Page 483.

Chapter 32: Regulatory and Legal Notices

Important Note on Modifications

Intentional or unintentional changes or modifications to the equipment must not be made unless under the express consent of the party responsible for compliance. Any such modifications could void the user's authority to operate the equipment and will void the manufacturer's warranty.

National and Regional Regulatory Notices

U.S. Federal Communication Commission (FCC) Notification

This device complies with Part 15 of the US FCC Rules and Regulations. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the US FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;
- Consult the dealer and/or experienced radio/TV technician for help.

FCC IDs and the specific configurations covered are listed in Table 83.

Table 83: US FCC IDs and Industry Canada certification numbers and covered configurations

FCC ID	Industry Canada Cert Number	Frequencies	Module Families	Antenna, Lens, or Reflector	Maximum Allowed Transmitter Output Power
ABZ89FC5809	109W-9000	8 MHz channels, centered on 906-924 MHz in 1 MHz increments (within the 902-928 MHz ISM band)	9000 SM, AP	12 dBi integrated antenna	24 dBm (250 mW)
				10 dBi Maxrad Model # Z1681 (MP9027XFPT or Cambium AN900A) flat panel	26 dBm (390 mW)
				10 dBi Mars Model # MA-IS91-T2, flat panel	26 dBm (390 mW)
				10 dBi MTI Model # MT-2630003/N (MT-263003/N) flat panel	26 dBm (390 mW)
				17 dBi Last Mile Gear Cyclone 900-17H Yagi	18 dBm (63 mW)
			9000 Indoor SM	8 dBi integrated antenna (Indoor SM)	26 dBm (390 mW)
ABZ89FC5808	109W-2400	20 MHz channels, centered on 2415-2457.5 MHz in 2.5 MHz increments (within the 2400-2483.5 MHz ISM band)	2400 BH, SM, AP	8 dBi internal	28 dBm (630 mW)
			2400 BH, SM	8 dBi internal + 11 dB reflector	25 dBm (340 mW)
			2400 SM, AP	External	23 dBm (200 mW)
ABZ89FC3789	109W-5200	20 MHz channels, centered on 5275-5325 MHz in 5 MHz increments (within the 5250-5350 MHz U-NII band)	5200 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
			5200 BH SM, AP, only P10 Modules	7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
				7 dBi internal + 9 dB lens	14 dBm (25 mW)

FCC ID	Industry Canada Cert Number	Frequencies	Module Families	Antenna, Lens, or Reflector	Maximum Allowed Transmitter Output Power
ABZ89FC5807	109W-5210	20 MHz channels, centered on 5275-5325 MHz in 5 MHz increments (within the 5250-5350 MHz U-NII band)	5210 BH	7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
ABZ89FT7623	none	20 MHz channels, centered on 5495-5705 MHz in 5 MHz increments (within the 5470-5725 MHz U-NII band)	5400 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
				7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
				7 dBi internal + 9 dB lens	14 dBm (25 mW)
none	109W-5400	20 MHz channels, centered on 5495-5575 and 5675-5705 MHz in 5 MHz increments (within the 5470-5725 MHz U-NII band with 5600-5650 MHz excluded)	5400 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
				7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
				7 dBi internal + 9 dB lens	14 dBm (25 mW)
ABZ89FC5804	109W-5700	20 MHz channels, centered on 5735-5840 MHz in 5 MHz increments (within the 5725-5850 MHz ISM band)	5700 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
			5700 BH, SM	7 dBi internal + 18 dB reflector	23 dBm (200 mW)
				7 dBi internal + 10 dB lens	23 dBm (200 mW)
			5700 AP	7 dBi internal + 10 dB lens	19 dBm (80 mW)
			5700 SM, AP	External	23 dBm (200 mW)(
ABZ89FT7629	none	10 MHz channels, centered on 5476-5719 in 0.5 MHz increments (within the 5470-5725 MHz U-NII band)	5440 AP	17 dBi connectorized antenna (60° x 5° 3 dB beam width)	10 dBm (10 mW)
			5440 SM	17 dBi integrated antenna (18° x 18° 3 dB beam width)	10 dBm (10 mW)

Industry Canada (IC) Notification

This device complies with RSS-210 of Industry Canada. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Users should be cautioned to take note that in Canada high power radars are allocated as primary users (meaning they have priority) of 5250 – 5350 MHz and 5650 – 5850 MHz and these radars could cause interference and/or damage to license-exempt local area networks (LELAN).

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to RSS-210 of Industry Canada. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;
- Consult the dealer and/or experienced radio/TV technician for help.

To reduce potential radio interference to other users, the antenna type and its gain should be chosen so its Equivalent Isotropic Radiated Power (EIRP) is not more than that permitted for successful communication.

Industry Canada Certification Numbers and the specific configurations covered are listed in Table 83.

This device has been designed to operate with the antennas listed in Table 83 and having a maximum gain as shown in Table 83. Antennas not included or having a gain greater than as shown in Table 83 are strictly prohibited from use with this device. Required antenna impedance is 50 ohms.

Regulatory Requirements for CEPT Member States (www.cept.org)

When operated in accordance with the instructions for use, Cambium Canopy Wireless equipment operating in the 2.4 and 5.4 GHz bands is compliant with CEPT Recommendation 70-03 Annex 3 for Wideband Data Transmission and HIPERLANs. For compliant operation in the 2.4 GHz band, the transmit power (EIRP) from the built-in patch antenna and any associated reflector dish shall be no more than 100mW (20dBm). For compliant operation in the 5.4 GHz band, the transmit power (EIRP) from the built-in patch antenna and any associated reflector dish shall be no more than 1 W (30 dBm).

The following countries have completely implemented CEPT Recommendation 70-03 Annex 3A (2.4 GHz band):

- EU & EFTA countries**:** Austria, Belgium, Denmark, Spain, Finland, Germany, Greece, Iceland, Italy, Ireland, Liechtenstein, Luxembourg, Netherlands, Norway, Portugal, Switzerland, Sweden, UK
- New EU member states**:** Bulgaria, Czech Republic, Cyprus, Estonia, Hungary, Lithuania, Latvia, Malta, Poland, Slovenia, Slovakia
- Other non-EU & EFTA countries: Bosnia and Herzegovina, Turkey

The following countries have a limited implementation of CEPT Recommendation 70-03 Annex 3A:

- France – Outdoor operation at 100mW is only permitted in the frequency band 2400 to 2454 MHz;
  - Any outdoor operation in the band 2454 to 2483.5MHz shall not exceed 10mW (10dBm);
  - Indoor operation at 100mW (20dBm) is permitted across the band 2400 to 2483.5 MHz
- French Overseas Territories:
  - Guadeloupe, Martinique, St Pierre et Miquelon, Mayotte – 100mW indoor & outdoor is allowed
  - Réunion and Guyana – 100mW indoor, no operation outdoor in the band 2400 to 2420MHz
- Italy – If used outside own premises, general authorization required
- Luxembourg - General authorization required for public service
- Romania – Individual license required. T/R 22-06 not implemented

Cambium Canopy Radios operating in the 2400 to 2483.5MHz band are categorized as “Class 2” devices within the EU and are marked with the class identifier symbol , denoting that national restrictions apply (for example, France). The French restriction in the 2.4 GHz band will be removed in 2011.

This 2.4 GHz equipment is “CE” marked to show compliance with the European Radio & Telecommunications Terminal Equipment (R&TTE) directive 1999/5/EC. The relevant Declaration of Conformity can be found at http://www.cambiumnetworks.com/doc.php.

Where necessary, the end user is responsible for obtaining any National licenses required to operate this product and these must be obtained before using the product in any particular country. However, for CEPT member states, 2.4 GHz Wideband Data Transmission equipment has been designated exempt from individual licensing under decision ERC/DEC(01)07. For EU member states, RLAN equipment in both the 2.4 & 5.4GHz bands is exempt from individual licensing under Commission Recommendation 2003/203/EC. Contact the appropriate national administrations for details on the conditions of use for the bands in question and any exceptions that might apply. Also see www.ero.dk for further information.

Cambium Canopy Radio equipment operating in the 5470 to 5725 MHz band are categorized as "Class 1" devices within the EU in accordance with ECC DEC(04)08 and are "CE" marked CE to show compliance with the European Radio & Telecommunications Terminal Equipment (R&TTE) directive 1999/5/EC. The relevant Declaration of Conformity can be found at http://www.cambiumnetworks.com/doc.php.

A European Commission decision, implemented by Member States on 31 October 2005, makes the frequency band 5470-5725 MHz available in all EU Member States for wireless access systems. Under this decision, the designation of Canopy 5.4GHz products become "Class 1 devices" and these do not require notification under article 6, section 4 of the R&TTE Directive. Consequently, these 5.4GHz products are only marked with the CE symbol and may be used in any member state.

For further details, see http://europa.eu.int/information_society/policy/radio_spectrum/ref_documents/index_en.htm

European Union Notification for 5.7 GHz Product

The 5.7 GHz connectorized product is a two-way radio transceiver suitable for use in Broadband Wireless Access System (WAS), Radio Local Area Network (RLAN), or Fixed Wireless Access (FWA) systems. It is a Class 2 device and uses operating frequencies that are not harmonized throughout the EU member states. The operator is responsible for obtaining any national licenses required to operate this product and these must be obtained before using the product in any particular country.

This equipment is marked CE ! 0977 to show compliance with the European R&TTE directive 1999/5/EC.

The relevant Declaration of Conformity can be found at http://www.cambiumnetworks.com/doc.php.

Equipment Disposal

Waste (Disposal) of Electronic and Electric Equipment

Please do not dispose of Electronic and Electric Equipment or Electronic and Electric Accessories with your household waste. In some countries or regions, collection systems have been set up to handle waste of electrical and electronic equipment. In European Union countries, please contact your local equipment supplier representative or service center for information about the waste collection system in your country.

EU Declaration of Conformity for RoHS Compliance

Cambium hereby, declares that these Cambium products are in compliance with the essential requirements and other relevant provisions of Directive 2002/95/EC, Restriction of the use of certain Hazardous Substances (RoHS) in electrical and electronic equipment.

The relevant Declaration of Conformity can be found at http://www.cambiumnetworks.com/doc.php.

UK Notification

The 5.7 GHz connectorized product has been notified for operation in the UK, and when operated in accordance with instructions for use it is compliant with UK Interface Requirement IR2007. For UK use, installations must conform to the requirements of IR2007 in terms of EIRP spectral density against elevation profile above the local horizon in order to protect Fixed Satellite Services. The frequency range 5795-5815 MHz is assigned to Road Transport & Traffic Telematics (RTTT) in the U.K. and shall not be used by FWA systems in order to protect RTTT devices. UK licensing specifies that radiolocation services shall be protected by a Dynamic Frequency Selection (DFS) mechanism to prevent co-channel operation in the presence of radar signals.

Belgium Notification

Belgium national restrictions in the 2.4 GHz band include

- EIRP must be lower then 100 mW
- For crossing the public domain over a distance > 300m the user must have the authorization of the BIPT.
- No duplex working

Luxembourg Notification

For the 2.4 GHz band, point-to-point or point-to-multipoint operation is only allowed on campus areas. 5.4GHz products can only be used for mobile services.

Czech Republic Notification

2.4 GHz products can be operated in accordance with the Czech General License No. GL-12/R/2000.

5.4 GHz products can be operated in accordance with the Czech General License No. GL-30/R/2000.

Norway Notification

Use of the frequency bands 5725-5795 / 5815-5850 MHz are authorized with maximum radiated power of 4 W EIRP and maximum spectral power density of 200 mW/MHz. The radio equipment shall implement Dynamic Frequency Selection (DFS) as defined in Annex 1 of ITU-R Recommendation M.1652 / EN 301 893. Directional antennae with a gain up to 23 dBi may be used for fixed point-to-point links. The power flux density at the border between Norway and neighboring states shall not exceed – 122.5 dBW/m^2 measured with a reference bandwidth of 1 MHz.

Canopy 5.7 GHz connectorized products have been notified for use in Norway and are compliant when configured to meet the above National requirements. Users shall ensure that DFS functionality is enabled, maximum EIRP respected for a 20 MHz channel, and that channel spacings comply with the allocated frequency band to protect Road Transport and Traffic Telematics services (for example, 5735, 5755, 5775 or 5835 MHz are suitable carrier frequencies). Note that for directional fixed links, TPC is not required, conducted transmit power shall not exceed 30 dBm, and antenna gain is restricted to 23 dBi (maximum of 40W from the Canopy 5.7 GHz connectorized products).

Italy Notification

In Italy, there is a regulation which requires a general authorization of any 5.4 GHz radio link which is used outside the operator's own premises. It is the responsibility of the installer or operator to have the link authorized. Details may be found at:

http://www.sviluppoeconomico.gov.it/index.php?option=com_content&view=article&idmenu=672&idarea1=593&andor=AND&idarea2=1052&id=68433&sectionid=1,16&viewType=1&showMenu=1&showCat=1&idarea3=0&andorcat=AND&partebassaType=0&idareaCalendario1=0&MvediT=1&idarea4=0&showArchiveNewsBotton=0&directionidUser=0

The form to be used for general authorization may be found at:

http://www.sviluppoeconomico.gov.it/images/stories/mise_extra/Allegato%20n19.doc

Greece Notification

The outdoor use of 5470-5725MHz is under license of EETT but is being harmonized according to the CEPT Decision ECC/DEC/(04) 08, of 9th July. End users are advised to contact the EETT to determine the latest position and obtain any appropriate licenses.

Brazil Notification

Local regulations do not allow the use of 900 MHz, 2.4 GHz, or 5.2 GHz Canopy modules in Brazil.

For compliant operation of an AP in the 5.7 GHz band, the Equivalent Isotropic Radiated Power from the built-in patch antenna and any associated reflector dish or LENS shall not exceed 36 dBm (4 W). When using the passive reflector (18 dB), transmitter output power must be configured no higher than 11 dBm. When using the LENS (10 dB at 5.7 GHz), transmitter output power must be configured no higher than 19 dBm.

For compliant operation in the 5.4 GHz band, the Equivalent Isotropic Radiated Power from the built-in patch antenna and any associated reflector dish or LENS shall not exceed 30 dBm (1 W). When using the passive reflector (18 dB), transmitter output power must be configured no higher than 5 dBm. When using the LENS (9 dB at 5.4 GHz), transmitter output power must be configured no higher than 14 dBm. When not using the passive reflector or the LENS, the transmitter output power of the radio must be configured no higher than 23 dBm.

The operator is responsible for enabling the DFS feature on any Canopy 5.4 GHz radio by setting the Region Code to “Brazil”, including after the module is reset to factory defaults.

Important Note: This equipment operates as a secondary application, so it has no rights against harmful interference, even if generated by similar equipment, and cannot cause harmful interference on systems operating as primary applications.

Australia Notification

900 MHz modules must be set to transmit and receive only on center channels of 920, 922, or 923 MHz so as to stay within the ACMA approved band of 915 MHz to 928 MHz for the class license and not interfere with other approved users.

After taking into account antenna gain (in dBi), 900 MHz modules’ transmitter output power (in dBm) must be set to stay within the legal regulatory limit of 30 dBm (1 W) EIRP for this 900 MHz frequency band.

Labeling and Disclosure Table for China

The People's Republic of China requires that Cambium's products comply with China Management Methods (CMM) environmental regulations. (China Management Methods refers to the regulation *Management Methods for Controlling Pollution by Electronic Information Products*.) Two items are used to demonstrate compliance; the label and the disclosure table.

The label is placed in a customer visible position on the product.

- Logo 1 means that the product contains no substances in excess of the maximum concentration value for materials identified in the China Management Methods regulation.
- Logo 2 means that the product may contain substances in excess of the maximum concentration value for materials identified in the China Management Methods regulation, and has an Environmental Friendly Use Period (EFUP) in years, fifty years in the example shown.

Logo 1 Logo 2

The Environmental Friendly Use Period (EFUP) is the period (in years) during which the Toxic and Hazardous Substances (T&HS) contained in the Electronic Information Product (EIP) will not leak or mutate causing environmental pollution or bodily injury from the use of the EIP. The EFUP indicated by the Logo 2 label applies to a product and all its parts. Certain field-replaceable parts, such as battery modules, can have a different EFUP and are marked separately.

The Disclosure Table is intended only to communicate compliance with China requirements; it is not intended to communicate compliance with EU RoHS or any other environmental requirements.

Table 84: Disclosure Table for China

部件名称	有毒有害物质或元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴□苯 (PBB)	多溴二苯□ (PBDE)
金属部件	×	○	×	×	○	○
□路模□	×	○	×	×	○	○
□□及□□组件	×	○	×	×	○	○
塑料和聚合物部件	○	○	○	○	○	×
表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T11363-2006 标准规定的限量要求以下。						

表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T11363-2006 标准规定的限量要求。

RF Exposure

For important information on RF exposure and separation distances see Section Exposure Separation Distances, on Page 174.

Legal Notices

Software License Terms and Conditions

ONLY OPEN THE PACKAGE, OR USE THE SOFTWARE AND RELATED PRODUCT IF YOU ACCEPT THE TERMS OF THIS LICENSE. BY BREAKING THE SEAL ON THIS DISK KIT / CDROM, OR IF YOU USE THE SOFTWARE OR RELATED PRODUCT, YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT USE THE SOFTWARE OR RELATED PRODUCT; INSTEAD, RETURN THE SOFTWARE TO PLACE OF PURCHASE FOR A FULL REFUND. THE FOLLOWING AGREEMENT IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR ENTITY), AND CAMBIUM, INC. (FOR ITSELF AND ITS LICENSORS). THE RIGHT TO USE THIS PRODUCT IS LICENSED ONLY ON THE CONDITION THAT YOU AGREE TO THE FOLLOWING TERMS.

Now, therefore, in consideration of the promises and mutual obligations contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby mutually acknowledged, you and Cambium agree as follows:

Grant of License. Subject to the following terms and conditions, Cambium, Inc., grants to you a personal, revocable, non-assignable, non-transferable, non-exclusive and limited license to use on a single piece of equipment only one copy of the software contained on this disk (which may have been pre-loaded on the equipment)(Software). You may make two copies of the Software, but only for backup, archival, or disaster recovery purposes. On any copy you make of the Software, you must reproduce and include the copyright and other proprietary rights notice contained on the copy we have furnished you of the Software.

Ownership. Cambium (or its supplier) retains all title, ownership and intellectual property rights to the Software and any copies,

including translations, compilations, derivative works (including images) partial copies and portions of updated works. The Software is Cambium's (or its supplier's) confidential proprietary information. This Software License Agreement does not convey to you any interest in or to the Software, but only a limited right of use. You agree not to disclose it or make it available to anyone without Cambium's written authorization. You will exercise no less than reasonable care to protect the Software from unauthorized disclosure. You agree not to disassemble, decompile or reverse engineer, or create derivative works of the Software, except and only to the extent that such activity is expressly permitted by applicable law.

Termination. This License is effective until terminated. This License will terminate immediately without notice from Cambium or judicial resolution if you fail to comply with any provision of this License. Upon such termination you must destroy the Software, all accompanying written materials and all copies thereof, and the sections entitled Limited Warranty, Limitation of Remedies and Damages, and General will survive any termination.

Limited Warranty. Cambium warrants for a period of ninety (90) days from Cambium's or its customer's shipment of the Software to you that (i) the disk(s) on which the Software is recorded will be free from defects in materials and workmanship under normal use and (ii) the Software, under normal use, will perform substantially in accordance with Cambium's published specifications for that release level of the Software. The written materials are provided "AS IS" and without warranty of any kind. Cambium's entire liability and your sole and exclusive remedy for any breach of the foregoing limited warranty will be, at Cambium's option, replacement of the disk(s), provision of downloadable patch or replacement code, or refund of the unused portion of your bargained for contractual benefit up to the amount paid for this Software License.

THIS LIMITED WARRANTY IS THE ONLY WARRANTY PROVIDED BY CAMBIUM, AND CAMBIUM AND ITS LICENSORS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OF IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. CAMBIUM DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. NO ORAL OR WRITTEN REPRESENTATIONS MADE BY CAMBIUM OR AN AGENT THEREOF SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. CAMBIUM DOES NOT WARRANT ANY SOFTWARE THAT HAS BEEN OPERATED IN EXCESS OF SPECIFICATIONS, DAMAGED, MISUSED, NEGLECTED, OR IMPROPERLY INSTALLED. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Limitation of Remedies and Damages. Regardless of whether any remedy set forth herein fails of its essential purpose, IN NO EVENT SHALL CAMBIUM OR ANY OF THE LICENSORS, DIRECTORS, OFFICERS, EMPLOYEES OR AFFILIATES OF THE FOREGOING BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL OR SIMILAR DAMAGES WHATSOEVER (including, without limitation, damages for loss of business profits, business interruption, loss of business information and the like), whether foreseeable or unforeseeable, arising out of the use or inability to use the Software or accompanying written materials, regardless of the basis of the claim and even if Cambium or a Cambium representative has been advised of the possibility of such damage. Cambium's liability to you for direct damages for any cause whatsoever, regardless of the basis of the form of the action, will be limited to the price paid for the Software that caused the damages. THIS LIMITATION WILL NOT APPLY IN CASE OF PERSONAL INJURY ONLY WHERE AND TO THE EXTENT THAT APPLICABLE LAW REQUIRES SUCH LIABILITY. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Maintenance and Support. Cambium shall not be responsible for maintenance or support of the software. By accepting the license granted under this agreement, you agree that Cambium will be under no obligation to provide any support, maintenance or service in connection with the Software or any application developed by you. Any maintenance and support of the Related Product will be provided under the terms of the agreement for the Related Product.

Transfer. In the case of software designed to operate on Cambium equipment, you may not transfer the Software to another party except: (1) if you are an end-user, when you are transferring the Software together with the Cambium equipment on which it operates; or 2) if you are a Cambium licensed distributor, when you are transferring the Software either together with such Cambium equipment or are transferring the Software as a licensed duly paid for upgrade, update, patch, new release, enhancement or replacement of a prior version of the Software. If you are a Cambium licensed distributor, when you are transferring the Software as permitted herein, you agree to transfer the Software with a license agreement having terms and conditions no less restrictive than those contained herein. You may transfer all other Software, not otherwise having an agreed restriction on transfer, to another party. However, all such transfers of Software are strictly subject to the conditions precedent that the other party agrees to accept the terms and conditions of this License, and you destroy any copy of the Software you do not transfer to that party. You may not sublicense or otherwise transfer, rent or lease the Software without our written consent. You may not transfer the Software in violation of any laws, regulations, export controls or economic sanctions imposed by the US Government.

Right to Audit. Cambium shall have the right to audit annually, upon reasonable advance notice and during normal business hours, your records and accounts to determine compliance with the terms of this Agreement.

Export Controls. You specifically acknowledge that the software may be subject to United States and other country export control laws. You shall comply strictly with all requirements of all applicable export control laws and regulations with respect to all such software and materials.

US Government Users. If you are a US Government user, then the Software is provided with "RESTRICTED RIGHTS" as set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights clause at FAR 52 227-19 or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, as applicable.

Disputes. You and Cambium hereby agree that any dispute, controversy or claim, except for any dispute, controversy or claim involving intellectual property, prior to initiation of any formal legal process, will be submitted for non-binding mediation, prior to initiation of any formal legal process. Cost of mediation will be shared equally. Nothing in this Section will prevent either party from resorting to judicial proceedings, if (i) good faith efforts to resolve the dispute under these procedures have been unsuccessful, (ii) the dispute, claim or controversy involves intellectual property, or (iii) interim relief from a court is necessary to prevent serious and irreparable injury to that party or to others.

General. Illinois law governs this license. The terms of this license are supplemental to any written agreement executed by both parties regarding this subject and the Software Cambium is to license you under it, and supersedes all previous oral or written communications between us regarding the subject except for such executed agreement. It may not be modified or waived except in writing and signed by an officer or other authorized representative of each party. If any provision is held invalid, all other provisions shall remain valid, unless such invalidity would frustrate the purpose of our agreement. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent action in the event of future breaches.

Hardware Warranty in U.S.

Cambium U.S. offers a warranty covering a period of one year from the date of purchase by the customer. If a product is found defective during the warranty period, Cambium will repair or replace the product with the same or a similar model, which may be a reconditioned unit, without charge for parts or labor.

Limit of Liability

IN NO EVENT SHALL CAMBIUM BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF CAMBIUM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply to you.) IN NO CASE SHALL CAMBIUM'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

Chapter 33: Additional Resources

Cambium provides two additional resources where you can raise questions and find answers:

- Community Forums at http://www.cambiumnetworks.com/forum/

  This resource facilitates communication with other users and with authorized Canopy experts. Available forums include General Discussion, Network Monitoring Tools, and Suggestions.

- Canopy Knowledge Base at http://www.cambiumnetworks.com/forum/viewforum.php?f=31&sid=cbc5d7149db9aa7c6477371db4494134.

  This resource facilitates exploration and searches, provides recommendations, and describes tools. Available categories include
  - General (Answers to general questions provide an overview of the Canopy system.)
  - Product Alerts
  - Helpful Hints
  - FAQs (frequently asked questions)
  - Hardware Support
  - Software Support
  - Tools

Glossary

~.	The command that terminates an SSH Secure Shell session to another server. Used on the Bandwidth and Authentication Manager (BAM) master server in the database replication setup.
10Base-T	Technology in Ethernet communications that can deliver 10 Mb of data across 328 feet (100 meters) of CAT 5 cable.
100Base-TX	Technology in Ethernet communications that can deliver 100 Mb of data across 328 feet (100 meters) of CAT 5 cable.
169.254.0.0	Gateway IP address default in Cambium fixed wireless broadband IP network modules.
169.254.1.1	IP address default in Cambium fixed wireless broadband IP network modules.
169.254.x.x	IP address default in Microsoft and Apple operating systems without a DHCP (Dynamic Host Configuration Protocol) server.
255.255.0.0	Subnet mask default in Cambium fixed wireless broadband IP network modules and in Microsoft and Apple operating systems.
802.3	An IEEE standard that defines the contents of frames that are transferred through Ethernet connections. Each of these frames contains a preamble, the address to which the frame is sent, the address that sends the frame, the length of the data to expect, the data, and a checksum to validate that no contents were lost.
802.11	The IEEE standard for wireless local area networks.
802.15	The IEEE standard for wireless personal area networks.
AAA	Authentication, Authorization, and Accounting
Access Point Cluster	Two to six Access Point Modules that together distribute network or Internet services to a community of 1,200 or fewer subscribers. Each Access Point Module covers a 60° sector. This cluster covers as much as 360°. Also known as AP cluster.
Access Point Module	Also known as AP. One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.
ACT/4	Second-from-left LED in the module. In the operating mode, this LED is lit when data activity is present on the Ethernet link. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Activate	To provide feature capability to a module, but not to *enable* (turn on) the feature in the module. See also Enable.
Address Resolution Protocol	Protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html.

Advanced Encryption Standard (AES)	Over-the-air link option that provides extremely secure wireless connections. Advanced Encryption Standard (AES) uses 128-bit secret keys as directed by the government of the U.S.A. AES is not exportable and requires a special AP to process the large keys.
AES	See Advanced Encryption Standard.
Aggregate Throughput	The sum of the throughputs in the uplink and the downlink.
AP	Access Point Module. One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.
APA	Access Point module address.
Apache	A trademark of Apache Software Foundation, used with permission.
APAS	Access Point Authentication Server. Licensed to authenticate SMs that attempt to register to it. The AP licensed as APAS may or may not have authentication *enabled* (turned on). See also Activate and Enable.
API	Application programming interface for web services that supports Prizm integration with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system.
APs MIB	Management Information Base file that defines objects that are specific to the Access Point Module or Backhaul timing master. See also Management Information Base.
ARP	Address Resolution Protocol. A protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html.
ASN.1	Abstract Syntax Notation One language. The format of the text files that compose the Management Information Base.
Attenuation	Reduction of signal strength caused by the travel from the transmitter to the receiver, and caused by any object between. In the absence of objects between, a signal that has a short wavelength experiences a high degree of attenuation nevertheless.
Authentication Key	Software key that correlates to the random number that the Bandwidth and Authentication Manager (BAM) server generates and sends in a challenge through the AP to the SM. The network operator can create and, at some security risk, send this key over the air to the SM. The SQL database in the BAM server correlates this key to QoS information about the SM. The format of this key is 32 hexadecimal characters of 0 to 9 and a to f, padded with leading zeroes in Release 4.2.3 and later. This key must be unique to the individual SM.

Backhaul Module	Also known as BH. A module that provides point-to-point connectivity as either a standalone link or a link to an Access Point cluster through a selected Access Point Module. See also Backhaul Timing Master and Backhaul Timing Slave.
Backhaul Timing Master	Backhaul Module that sends network timing (synchronization) to another Backhaul Module, which serves as the Backhaul timing slave.
Backhaul Timing Slave	Backhaul Module that receives network timing (synchronization) from another Backhaul Module, which serves as the Backhaul timing master.
BAM	Bandwidth and Authentication Manager. The subsystem of Prizm that manages sets of bandwidth, high-priority channel, and VLAN settings individually for registered Subscriber Modules. This software also provides secure Subscriber Module authentication and user-specified encryption keys.
BER	Bit Error Rate. The ratio of incorrect data received to correct data received.
BH	Backhaul Module. A module that provides point-to-point connectivity as either a standalone link or a link to an Access Point cluster through a selected Access Point Module.
Bit Error Rate	Ratio of incorrect data received to correct data received.
Box MIB	Management Information Base file that defines module-level objects. See also Management Information Base.
BRAID	Stream cipher that the TIA (Telecommunications Industry Association) has standardized. The secret keys in both modules communicate with each other to establish the Data Encryption Standard key. See Data Encryption Standard.
Bridge	Network element that uses the physical address (not the logical address) of another to pass data. The bridge passes the data to either the destination address, if found in the simple routing table, or to all network segments other than the one that transmitted the data. Modules are Layer 2 bridges except that, where NAT is enabled for an SM, the SM is a Layer 3 switch. Compare to Switch and Router, and see also NAT.
Bridge Entry Timeout Field	Value that the operator sets as the maximum interval for no activity with another module, whose MAC address is the Bridge Entry. This interval should be longer than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.
Buckets	Theoretical data repositories that can be filled at preset rates or emptied when preset conditions are experienced, such as when data is transferred.
Burst	Preset amount limit of data that may be continuously transferred.

C/I Ratio	Ratio of intended signal (carrier) to unintended signal (interference) received.
Canopy	A trademark of Cambium, Inc.
Carrier-to-interference Ratio	Ratio of intended reception to unintended reception.
CarSenseLost Field	This field displays how many carrier sense lost errors occurred on the Ethernet controller.
CAT 5 Cable	Cable that delivers Ethernet communications from module to module. Later modules auto-sense whether this cable is wired in a straight-through or crossover scheme.
chkconfig	A command that the Linux® operating system accepts to enable MySQL® and Apache™ Server software for various run levels of the mysqld and httpd utilities.
CIR	See Committed Information Rate.
Cluster Management Module	Module that provides power, GPS timing, and networking connections for an AP cluster. Also known as CMM. If this CMM is connected to a Backhaul Module, then this CMM is the central point of connectivity for the entire site.
CMM	Cluster Management Module. A module that provides power, GPS timing, and networking connections for an Access Point cluster. If this CMM is connected to a Backhaul Module (BH), then this CMM is the central point of connectivity for the entire site.
CodePoint	See DiffServ.
Color Code Field	Module parameter that identifies the other modules with which communication is allowed. The range of values is 0 to 255. When set at 0, the Color Code does not restrict communications with any other module.
Committed Information Rate (CIR)	For an SM or specified group of SMs, a level of bandwidth that can be guaranteed to never fall below a specified minimum. In the Cambium implementation, this is controlled by the Low Priority Uplink CIR, Low Priority Downlink CIR, High Priority Uplink CIR, and High Priority Downlink CIR parameters.
Community String Field	Control string that allows a network management station to access MIB information about the module.
CPE	Customer premises equipment.
CRCError Field	This field displays how many CRC errors occurred on the Ethernet controller.
CRM	Customer relationship management system.

Data Encryption Standard Over-the-air link option that uses secret 56-bit keys and 8 parity bits. Data Encryption Standard (DES) performs a series of bit permutations, substitutions, and recombination operations on blocks of data.

Date of Last Transaction A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the date of the most recent authentication attempt by the SM. Expressed in the database output as DLT.

Dell A trademark of Dell, Inc.

Demilitarized Zone Internet Protocol area outside of a firewall. Defined in RFC 2647. See http://www.faqs.org/rfcs/rfc2647.html.

DES Data Encryption Standard. An over-the-air link option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data.

Desensed Received an undesired signal that was strong enough to make the module insensitive to the desired signal.

DFS See Dynamic Frequency Selection.

DHCP Dynamic Host Configuration Protocol, defined in RFC 2131. Protocol that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the system. See http://www.faqs.org/rfcs/rfc2131.html. See also Static IP Address Assignment.

Diffraction Partial obstruction of a signal. Typically diffraction attenuates a signal so much that the link is unacceptable. However, in some instances where the obstruction is very close to the receiver, the link may be acceptable.

DiffServ Differentiated Services, consistent with RFC 2474. A byte in the type of service (TOS) field of packets whose values correlates to the channel on which the packet should be sent. The value is a numeric code point. Cambium modules map each of 64 code points to values of 0 through 7. Three of these code points have fixed values, and the remaining 61 are settable. Values of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities. (However, configuring DiffServ does not automatically enable the VLAN feature.) Among the settable parameters, the values are set in the AP for all downlinks within the sector and in the SM for each uplink.

Disable To turn off a feature in the module after both the feature activation file has *activated* the module to use the feature and the operator has *enabled* the feature in the module. See also Activate and Enable.

DLT	Date of last transaction. A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the date of the most recent authentication attempt by the SM.
DMZ	Demilitarized Zone as defined in RFC 2647. An Internet Protocol area outside of a firewall. See http://www.faqs.org/rfcs/rfc2647.html.
Dynamic Frequency Selection (DFS)	A requirement in certain countries and regions for systems to detect interference from other systems, notably radar systems, and to avoid co-channel operation with these systems. See also Region Code.
Dynamic Host Configuration Protocol	See DHCP.
Electronic Serial Number	Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number. Same as MAC Address.
Element Pack	A license for Prizm management of a multi-point sector and covers the AP and up to 200 SMs or a backhaul link.
Enable	To turn on a feature in the module after the feature activation file has *activated* the module to use the feature. See also Activate.
Engine	Bandwidth and Authentication Manager (BAM) interface to the AP and SMs. Unique sets of commands are available on this interface to manage parameters and user access. Distinguished from SSE. See also SSE.
ESN	Electronic Serial Number. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number. Same as MAC Address.
ESN Data Table	Table in which each row identifies data about a single SM. In tab-separated fields, each row stores the ESN, authentication key, and QoS information that apply to the SM. The operator can create and modify this table. This table is both an input to and an output from the Bandwidth and Authentication Manager (BAM) SQL database, and should be identically input to redundant BAM servers.
/etc/services	File that stores telnet ports on the Bandwidth and Authentication Manager (BAM) server.
EthBusErr Field	This field displays how many Ethernet bus errors occurred on the Ethernet controller.
Ethernet Protocol	Any of several IEEE standards that define the contents of frames that are transferred from one network element to another through Ethernet connections.

Fade Margin	The difference between strength of the received signal and the strength that the receiver requires for maintaining a reliable link. A higher fade margin is characteristic of a more reliable link. Standard operating margin.
FCC	Federal Communications Commission of the U.S.A.
Feature Activation Key	Software key file whose file name includes the ESN of the target module. When installed on the module, this file *activates* the module to have the feature *enabled* or disabled in a separate operator action.
Field-programmable Gate Array	Array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.
File Transfer Protocol	Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. Defined in RFC 959. See http://www.faqs.org/rfcs/rfc959.html.
FPGA	Field-programmable Gate Array. An array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.
Frame Spreading	Transmission of a beacon in only frames where the receiver expects a beacon (rather than in every frame). This avoids interference from transmissions that are not intended for the receiver.
Frame Timing Pulse Gated Field	Toggle parameter that prevents or allows the module to continue to propagate GPS sync timing when the module no longer receives the timing.
Free Space Path Loss	Signal attenuation that is naturally caused by atmospheric conditions and by the distance between the antenna and the receiver.
Fresnel Zone	Space in which no object should exist that can attenuate, diffract, or reflect a transmitted signal before the signal reaches the target receiver.
FSK	Frequency Shift Keying, a variation of frequency modulation to transmit data, in which two or more frequencies are used.
FTP	File Transfer Protocol, defined in RFC 959. Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. See http://www.faqs.org/rfcs/rfc959.html.
Global Positioning System	Network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
GPS	Global Positioning System. A network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.

GPS/3	Third-from-left LED in the module. In the operating mode for an Access Point Module or Backhaul timing master, this LED is continuously lit as the module receives sync pulse. In the operating mode for a Subscriber Module or a Backhaul timing slave, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
GUI	Graphical user interface.
High-priority Channel	Channel that supports low-latency traffic (such as Voice over IP) over low-latency traffic (such as standard web traffic and file downloads). To recognize the latency tolerance of traffic, this channel reads the IPv4 Type of Service DiffServ Control Point (DSCP) bits. Enabling the high-priority channel reduces the maximum number of SMs that can be served in the sector.
HTTP	Hypertext Transfer Protocol, used to make the Internet resources available on the World Wide Web. Defined in RFC 2068. See http://www.faqs.org/rfcs/rfc2068.html.
ICMP	Internet Control Message Protocols defined in RFC 792, used to identify Internet Protocol (IP)-level problems and to allow IP links to be tested. See http://www.faqs.org/rfcs/rfc792.html.
indiscards count Field	How many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. (Some of these packets may have been discarded to increase buffer space.)
inerrors count Field	How many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
innucastpkts count Field	How many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.
inoctets count Field	How many octets were received on the interface, including those that deliver framing information.
Intel	A registered trademark of Intel Corporation.
inucastpkts count Field	How many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
inunknownprotos count Field	How many inbound packets were discarded because of an unknown or unsupported protocol.
IP	Internet Protocol defined in RFC 791. The Network Layer in the TCP/IP protocol stack. This protocol is applied to addressing, routing, and delivering, and re-assembling data packets into the Data Link layer of the protocol stack. See http://www.faqs.org/rfcs/rfc791.html.

IP Address	32-bit binary number that identifies a network element by both network and host. See also Subnet Mask.
IPv4	Traditional version of Internet Protocol, which defines 32-bit fields for data transmission.
ISM	Industrial, Scientific, and Medical Equipment radio frequency band, in the 900-MHz, 2.4-GHz, and 5.8-GHz ranges.
Jitter	Timing-based measure of the reception quality of a link. An acceptable link displays a jitter value between 0 and 4 for a 10-Mbps Backhaul timing slave in Release 4.0 and later, between 0 and 9 for a 20-Mbps Backhaul timing slave, or between 5 and 9 for any Subscriber Module or for a Backhaul timing slave in any earlier release. OFDM modules do not have this parameter.
L2TP over IPSec	Level 2 Tunneling Protocol over IP Security. One of several virtual private network (VPN) implementation schemes. Regardless of whether Subscriber Modules have the Network Address Translation feature (NAT) enabled, they support VPNs that are based on this protocol.
Late Collision Field	This field displays how many late collisions occurred on the Ethernet controller. A normal collision occurs during the first 512 bits of the frame transmission. A collision that occurs after the first 512 bits is considered a late collision. A late collision is a serious network problem because the frame being transmitted is discarded. A late collision is most commonly caused by a mismatch between duplex configurations at the ends of a link segment.
Latency Tolerance	Acceptable tolerance for delay in the transfer of data to and from a module.
Line of Sight	Wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.
Linux	A registered trademark of Linus Torvalds.
LNK/5	Furthest left LED in the module. In the operating mode, this LED is continuously lit when the Ethernet link is present. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Logical Unit ID	Final octet of the 4-octet IP address of the module.
LOS	Line of sight. The wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.
LUID	Logical Unit ID. The final octet of the 4-octet IP address of the module.

MAC Address	Media Access Control address. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
Management Information Base	Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).
Master	Designation that defines the role of a component relative to the role of another. This designation both applies to a Backhaul module that provides synchronization over the air to another Backhaul module (a Backhaul timing slave) and applies to a Bandwidth and Authentication Manager (BAM) server whose SQL database is automatically copied onto a redundant BAM server (BAM slave). In each case, the master is not a product. Rather, the master is the role that results from deliberate configuration steps.
Maximum Information Rate (MIR)	The cap applied to the bandwidth of an SM or specified group of SMs. In the Cambium implementation, this is controlled by the Sustained Uplink Data Rate, Uplink Burst Allocation, Sustained Downlink Data Rate, and Downlink Burst Allocation parameters.
Media Access Control Address	Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
MIB	Management Information Base. Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).
MIR	See Maximum Information Rate.
MySQL	A registered trademark of MySQL AB Company in the United States, the European Union, and other countries.
mysqladmin	A command to set the administrator and associated password on the Bandwidth and Authentication Manager (BAM) server.
mysql-server	Package group that enables the SQL Database Server application in the Red Hat® Linux® 9 operating system to provide SQL data for Bandwidth and Authentication Manager (BAM) operations.
NAT	Network Address Translation defined in RFC 1631. A scheme that isolates Subscriber Modules from the Internet. See http://www.faqs.org/rfcs/rfc1631.html.
NBI	See Northbound Interface.
NEC	National Electrical Code. The set of national wiring standards that are enforced in the U.S.A.

NetBIOS	Protocol defined in RFC 1001 and RFC 1002 to support an applications programming interface in TCP/IP. This interface allows a computer to transmit and receive data with another host computer on the network. RFC 1001 defines the concepts and methods. RFC 1002 defines the detailed specifications. See http://www.faqs.org/rfcs/rfc1001.html and http://www.faqs.org/rfcs/rfc1002.html.
Network Address Translation	Scheme that defines the Access Point Module as a proxy server to isolate registered Subscriber Modules from the Internet. Defined in RFC 1631. See http://www.faqs.org/rfcs/rfc1631.html.
Network Management Station	See NMS.
NMS	Network Management Station. A monitor device that uses Simple Network Management Protocol (SNMP) to control, gather, and report information about predefined network variables (objects). See also Simple Network Management Protocol.
Northbound Interface (NBI)	The interface within Prizm to higher-level systems. This interface consists of a Simple Network Management Protocol (SNMP) agent for integration with a network management system (NMS); a Simple Object Access Protocol (SOAP) XML-based application programming interface (API) for web services that supports integration with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system; and console automation that allows such higher-level systems to launch and appropriately display the PrizmEMS management console in a custom-developed GUI.
Object	Network variable that is defined in the Management Information Base.
OptiPlex	A trademark of Dell, Inc.
OSS	Operations support system, such as a customer relationship management (CRM), billing, or provisioning system. The application programming interface (API) for Prizm supports integrating Prizm with an OSS.
outdiscards count Field	How many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)
outerrrors count Field	How many outbound packets contained errors that prevented their transmission.
outnucastpkts count Field	How many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.
outoctets count Field	How many octets were transmitted out of the interface, including those that deliver framing information.

outucastpkts count Field	How many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.
Override Plug	Device that enables the operator to regain control of a module that has been locked by the No Remote Access feature, the 802.3 Link Disable feature, or a password or IP address that cannot be recalled. This device can be either fabricated on site or ordered.
Pentium	A registered trademark of Intel Corporation.
php-mysql	Package group that enables the Web Server application in the Red Hat® Linux® 9 operating system to provide data from the SQL Database Server application as PHP in the Bandwidth and Authentication Manager (BAM) GUI.
PMP	See Point-to-Multipoint Protocol.
Point-to-Multipoint Protocol	Defined in RFC 2178, which specifies that data that originates from a central network element can be received by all other network elements, but data that originates from a non-central network element can be received by only the central network element. See http://www.faqs.org/rfcs/rfc2178.html. Also referenced as PMP.
Point-to-Point Protocol	Standards that RFC 1661 defines for data transmittal on the Internet. Also known as PPP or PTP. See http://www.faqs.org/rfcs/rfc1661.html.
Power Control	Feature in Release 4.1 and later that allows the module to operate at less than 18 dB less than full power to reduce self-interference.
PPPoE	Point to Point Protocol over Ethernet. Supported on SMs for ◦ operators who use PPPoE in other parts of their network ◦ operators who want to deploy PPPoE to realize per-subscriber authentication, metrics, and usage control.
PPTP	Point to Point Tunneling Protocol. One of several virtual private network implementations. Regardless of whether the Network Address Translation (NAT) feature enabled, Subscriber Modules support VPNs that are based on this protocol.
Prizm	The software product that allows users to partition their entire networks into criteria-based subsets and independently monitor and manage those subsets. Prizm Release 1.0 and later includes a Northbound Interface to higher-level systems. Prizm integrates Bandwidth and Authentication Manager (BAM) functionality.
Protective Earth	Connection to earth (which has a charge of 0 volts). Also known as ground.

Proxy Server	Network computer that isolates another from the Internet. The proxy server communicates for the other computer, and sends replies to only the appropriate computer, which has an IP address that is not unique or not registered.
PTMP	See Point-to-Multipoint Protocol.
PTP	See Point-to-Point Protocol.
QoS	Quality of Service. A frame field that Bandwidth and Authentication Manager (BAM) provides to the AP and SM about the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields.
Quality of Service	A frame bit that Bandwidth and Authentication Manager (BAM) provides to the AP and SM the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields. Also known as QoS.
Quick Start	Interface page that requires minimal configuration for initial module operation.
Radio Signal Strength Indicator	Relative measure of the strength of a received signal. An acceptable link displays an Radio Signal Strength Indicator (RSSI) value of greater than 700.
RADIUS	Remote Authentication Dial In User Service
Random Number	Number that the Bandwidth and Authentication Manager (BAM) generates, invisible to both the SM and the network operator, to send to the SM as a challenge against an authentication attempt.
Reader	A registered trademark of Adobe Systems, Incorporated.
Recharging	Resumed accumulation of data in available data space (buckets). See Buckets.
Red Hat	A registered trademark of Red Hat, Inc.
Reflection	Change of direction and reduction of amplitude of a signal that encounters an object larger than the wavelength. Reflection may cause an additional copy of the wavelength to arrive after the original, unobstructed wavelength arrives. This causes partial cancellation of the signal and may render the link unacceptable. However, in some instances where the direct signal cannot be received, the reflected copy may be received and render an otherwise unacceptable link acceptable.

Region Code A parameter that offers multiple fixed selections, each of which automatically implements either the Dynamic Frequency Selection (DFS) standard that is required by law or regulatory to apply or no DFS, based on the frequency band range and the selected region.

Registrations MIB Management Information Base file that defines registrations for global items such as product identities and product components. See also Management Information Base.

repl-m A command that sets up the database replication process on a Bandwidth and Authentication Manager (BAM) master server, uses SFTP to copy both the database and the `repl-s` script to a BAM slave server, and remotely executes the `repl-s` script on the BAM slave server. See Master, Slave, `repl-s`, Secure Shell, and SFTP.

repl-s A command that sets up the database replication process on a Bandwidth and Authentication Manager (BAM) slave server. See Master, Slave, and `repl-m`.

RES Result. A field in the data that the `cmd show esn` command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server.

RetransLimitExp Field This field displays how many times the retransmit limit has expired.

RF Radio frequency. How many times each second a cycle in the antenna occurs, from positive to negative and back to positive amplitude.

RJ-11 Standard cable that is typically used for telephone line or modem connection.

RJ-45 Standard cable that is typically used for Ethernet connection. This cable may be wired as straight-through or as crossover. Later modules auto-sense whether the cable is straight-through or crossover.

Router Network element that uses the logical (IP) address of another to pass data to only the intended recipient. Compare to Switch and Bridge.

RPM Red Hat® Package Manager.

rpm A command that the Linux® operating system accepts to identify the version of Linux® software that operates on the Bandwidth and Authentication Manager (BAM) server.

RSSI Radio Signal Strength Indicator. A relative measure of the strength of a received signal. An acceptable link displays an RSSI value of greater than 700.

RxBabErr Field This field displays how many receiver babble errors occurred.

RxOverrun Field This field displays how many receiver overrun errors occurred on the Ethernet controller.

SDK	*PrizmEMS™ Software Development Kit (SDK)*—the document that provides server administrator tasks, GUI developer information for console automation that allows higher-level systems to launch and appropriately display the Prizm management console. The SDK also describes the how to define new element types and customize the Details views.
Secure Shell	A trademark of SSH Communications Security.
Self-interference	Interference with a module from another module in the same network.
SES/2	Third-from-right LED in the module. In the Access Point Module and Backhaul timing master, this LED is unused. In the operating mode for a Subscriber Module or a Backhaul timing slave, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Session Key	Software key that the SM and Bandwidth and Authentication Manager (BAM) separately calculate based on that both the authentication key (or the factory-set default key) and the random number. BAM sends the session key to the AP. Neither the subscriber nor the network operator can view this key. See also Random Number.
SFTP	Secure File Transfer Protocol.
Simple Network Management Protocol	Standard that is used for communications between a program (agent) in the network and a network management station (monitor). Defined in RFC 1157. See http://www.faqs.org/rfcs/rfc1157.html.
skey	Software key that correlates to the random number that the Bandwidth and Authentication Manager (BAM) server generates and sends in a challenge through the AP to the SM. The network operator can create and, at some security risk, send this key over the air to the SM. The SQL database in the BAM server correlates this key to QoS information about the SM. The format of this key is 32 hexadecimal characters of 0 to 9 and a to f. This key must be unique to the individual SM. Also known as authentication key.
Slave	Designation that defines the role of a component relative to the role of another. This designation both applies to a Backhaul slave that receives synchronization over the air from another Backhaul module (a Backhaul timing master) and applies to a redundant Bandwidth and Authentication Manager (BAM) server whose SQL database is automatically overwritten by a copy from the primary BAM server (BAM master). In each case, the slave is not a product. Rather, the slave is the role that results from deliberate configuration steps.
SM	Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.

SM MIB	Management Information Base file that defines objects that are specific to the Subscriber Module or Backhaul timing slave. See also Management Information Base.
SNMP	See Simple Network Management Protocol, defined in RFC 1157.
SNMP Trap	Capture of information that informs the network monitor through Simple Network Management Protocol of a monitored occurrence in the module.
SOAP	Simple Object Access Protocol (SOAP). The protocol that the Northbound Interface in Prizm uses to support integration of Prizm with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system
SSE	Bandwidth and Authentication Manager (BAM) interface to the SQL server. Unique sets of commands are available on this interface to manage the BAM SQL database and user access. Distinguished from Engine. See also Engine.
Standard Operating Margin	See Fade Margin.
Static IP Address Assignment	Assignment of Internet Protocol address that can be changed only manually. Thus static IP address assignment requires more configuration time and consumes more of the available IP addresses than DHCP address assignment does. RFC 2050 provides guidelines for the static allocation of IP addresses. See http://www.faqs.org/rfcs/rfc2050.html. See also DHCP.
su -	A command that opens a Linux® operating system session for the user `root`.
Subnet Mask	32-bit binary number that filters an IP address to reveal what part identifies the network and what part identifies the host. The number of subnet mask bits that are set to 1 indicates how many leading bits of the IP address identify the network. The number of subnet mask bits that are set 0 indicate how many trailing bits of the IP address identify the host.
Subscriber Module	Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.
Sustained Data Rate	Preset rate limit of data transfer.
Switch	Network element that uses the port that is associated with the physical address of another to pass data to only the intended recipient. Compare to Bridge and Router.

SYN/1	Second-from-right LED in the module. In the Access Point Module or Backhaul timing master, as in a registered Subscriber Module or Backhaul timing slave, this LED is continuously lit to indicate the presence of sync. In the operating mode for a Subscriber Module or Backhaul timing slave, this LED flashes on and to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Sync	GPS (Global Positioning System) absolute time, which is passed from one module to another. Sync enables timing that prevents modules from transmitting or receiving interference. Sync also provides correlative time stamps for troubleshooting efforts.
TCP	Alternatively known as Transmission Control Protocol or Transport Control Protocol. The Transport Layer in the TCP/IP protocol stack. This protocol is applied to assure that data packets arrive at the target network element and to control the flow of data through the Internet. Defined in RFC 793. See http://www.faqs.org/rfcs/rfc793.html.
tcp	Transport Control type of port. The system uses Port 3306:tcp for MySQL® database communications, Port 9080:tcp for SSE `telnet` communications, and Port 9090:tcp for Engine `telnet` communications.
TDD	Time Division Duplexing. Synchronized data transmission with some time slots allocated to devices transmitting on the uplink and some to the device transmitting on the downlink.
telnet	Utility that allows a client computer to update a server. A firewall can prevent the use of the `telnet` utility to breach the security of the server. See http://www.faqs.org/rfcs/rfc818.html, http://www.faqs.org/rfcs/rfc854.html and http://www.faqs.org/rfcs/rfc855.html.
Textual Conventions MIB	Management Information Base file that defines system-specific textual conventions. See also Management Information Base.
Time of Last Transaction	A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the time of day of the most recent authentication attempt by the SM. Expressed in the database output as TLT.
TLT	Time of last transaction. A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the time of day of the most recent authentication attempt by the SM.

TNAF	Total number of authentication requests failed. A field in the data that the `cmd show esn` command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field indicates how many times the SM (identified by ESN in the related data) attempted to authenticate but was denied by BAM.
TNAR	Total number of authentication requests. A field in the data that the `cmd show esn` command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field indicates how many times the SM (identified by ESN in the related data) attempted to authenticate, regardless of whether the attempt succeeded.
Tokens	Theoretical amounts of data. See also Buckets.
TOS	8-bit field in that prioritizes data in a IP transmission. See http://www.faqs.org/rfcs/rfc1349.html.
TxUnderrun Field	This field displays how many transmission-underrun errors occurred on the Ethernet controller.
UDP	User Datagram Protocol. A set of Network, Transport, and Session Layer protocols that RFC 768 defines. These protocols include checksum and address information but does not retransmit data or process any errors. See http://www.faqs.org/rfcs/rfc768.html.
udp	User-defined type of port.
U-NII	Unlicensed National Information Infrastructure radio frequency band, in the 5.1-GHz through 5.8-GHz ranges.
VID	VLAN identifier. See also VLAN.
VLAN	Virtual local area network. An association of devices through software that contains broadcast traffic, as routers would, but in the switch-level protocol.
VPN	Virtual private network for communication over a public network. One typical use is to connect remote employees, who are at home or in a different city, to their corporate network over the Internet. Any of several VPN implementation schemes is possible. SMs support L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) VPNs and PPTP (Point to Point Tunneling Protocol) VPNs, regardless of whether the Network Address Translation (NAT) feature enabled.